

1. Introduction

This Privacy Compliance Framework Policy (the "Policy") establishes BMC Helix's ("Helix") approach to compliance with European data protection law, including transfers of Personal Information between Helix affiliates ("Affiliates"). It is intended to uphold privacy commitments and ensure continued application of consistent and effective data protection standards across all Helix Affiliates in relation to the processing of Personal Information.

Helix must comply with and respect the Policy when collecting and using Personal Information. In particular, the Policy describes the standards that Affiliates must apply when they transfer Personal Information internationally to other Affiliates, whether Affiliates are transferring Personal Information for their own purposes or when providing services to a third-party controller.

Transfers of Personal Information take place between Affiliates during the normal course of business, and such information may be stored in centralized databases accessible by Affiliates from anywhere in the world.

The Policy applies to all Personal Information of past, current and potential employees, customers, resellers, suppliers, service providers and other third parties wherever it is collected and used in conjunction with Helix business activities and the administration of employment.

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

2. Scope and Compliance

This Policy is based on European data protection laws and standards and applies to Helix employees across all Helix Affiliates, regardless of geographic location. Employees are required to comply with this Policy as described in the Overview of Corporate Policies. The Policy also applies to Contingent Workers, contractors, business partners, managers of Helix's data repositories, and others who receive or process Personal Information.

3. Definitions

For the purposes of this Policy and unless otherwise specified, the following terms have the meaning set forth below:

- **Applicable law** means the laws applicable to the relevant processing, transfer, controller, processor, data subject, or service agreement context.

- **Privacy Compliance Framework, PCF or Policy** means this Policy to ensure data protection and privacy compliance worldwide, especially with regard to international transfers of Personal Information between Affiliates.
- **Helix or BMC Helix** means BMC Helix and its Affiliates subject to the Policy.
- **Client** means a third-party Controller or Processor on behalf and under the instructions of which Helix processes Personal Information, under the Policy and the applicable service agreement.
- **Competent Supervisory Authority** means the supervisory authority competent for the data exporter.
- **Controller** means a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Information.
- **Exporter** means an Affiliate based in Europe, and which transfers Personal Information to another Affiliate based in a third country.
- **Importer** means an Affiliate based in a third country to which Personal Information is transferred by another Affiliate based in Europe.
- **European Economic Area or “EEA”** means the Member States of the European Union (EU) and three countries of the European Free Trade Association (EFTA) (Iceland, Liechtenstein and Norway).
- **Europe** means the EEA and Switzerland.
- **GDPR** means Regulation (EU) 2016/679 of 27 April 2016, on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data, as amended from time to time.
- **Individual**, also designated as “data subject” under GDPR, means an identifiable natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
- **Personal Information**, also designated as “Personal Data” under GDPR, means any information relating to an identified or identifiable individual.
- **Processing** means any operation or set of operations which is performed on Personal Information or on sets of Personal Information, whether or not by automated means, such as collection,

recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

- **Processor** means a natural or legal person, public authority, agency or other body which processes Personal Information on behalf and under the instructions of a controller.
- **Request for Disclosure** means a legally binding request from a public authority (e.g., a law enforcement authority or state security body), including judicial authorities, acting under the laws of a third country not recognized by the European Commission as ensuring an adequate level of protection and requesting the disclosure of Personal Information transferred pursuant to this Policy.
- **Sensitive Personal Information** means Personal Information relating to an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health data, sex life, sexual orientation, criminal convictions and offenses.
- **Third country** means a country that is not a member of the EEA nor Switzerland.

4. Policy Statement

Helix Affiliates and their employees must comply with this Policy including the requirements set out in the appendices. Helix employees must take proper steps to ensure that transfers of Personal Information between Helix Affiliates and third parties are carried out in accordance with this framework, to ensure that such transfers are completed in a secure and lawful manner.

This Policy does not replace any specific data protection requirements that might apply to a business area or function. Furthermore, this Policy does not pre-empt country specific privacy laws and filing requirements.

5. Roles and Responsibilities

- A. Managers are responsible for ensuring that employees who report to them and/or contractors who provide services to them are aware of the requirements of this Policy and oversee processes and contractor and employee activities to ensure compliance.
- B. Employees, contingent workers, contractors, business partners and suppliers are responsible for understanding the requirements of this Policy as it relates to Personal Information processed on behalf of Helix or entrusted to Helix and to ensure that Personal Information is processed in compliance with all aspects of the Policy.

6. Document Information

Last Review Date	September, 2026
------------------	-----------------

PART I: PRIVACY COMPLIANCE FRAMEWORK BACKGROUND

WHAT IS DATA PROTECTION LAW?

Data protection law gives people certain rights in connection with the way in which their Personal Information is used. If organizations do not comply with data protection law, they may be subject to sanctions and penalties imposed by supervisory authorities and courts. When Affiliates collect and use Personal Information of their past, current and potential employees, customers, resellers, suppliers, service providers and other third parties, this activity, and Personal Information in question, is covered and regulated by data protection law.

Under data protection law, when an organization collects, uses or transfers Personal Information for its own purposes, that organization 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 organization processes Personal Information on behalf of a third party (for example, to provide a service), that organization is deemed to be a processor of the information and the third party will be primarily responsible for meeting the legal requirements. The Policy describes how Helix will comply with data protection law in respect of processing undertaken in its capacity as both a controller and as a processor.

HOW DOES EUROPEAN DATA PROTECTION LAW AFFECT HELIX INTERNATIONALLY?

European data protection law prohibits the transfer of Personal Information to countries outside Europe that do not ensure an adequate level of data protection. Some of the countries in which Helix operates are not regarded by European supervisory authorities as providing an adequate level of protection for individuals' data privacy rights.

WHAT IS HELIX DOING ABOUT IT?

Affiliates must take proper steps to ensure that they use Personal Information on an international basis in a safe and lawful manner. The purpose of the Policy, therefore, is to set out a framework to satisfy the standards contained in European data protection law and, as a result, support an adequate level of protection for all Personal Information used and collected in Europe and transferred from Affiliates within Europe to Affiliates outside Europe.

Affiliates will apply the Policy globally, and in all cases where Affiliates process Personal Information both manually and by automatic means, when Personal Information relates to past, current and potential employees, customers, resellers, suppliers, service providers and other third parties.

The Policy applies to all Affiliates and their employees worldwide and requires that:

- Affiliates who process Personal Information as a controller must comply with Part II of the Policy together with the practical procedures set out in the appendices in Part IV of the Policy.
- Affiliates who process Personal Information to provide services to a third party as a processor or who provide a service to other Affiliates as a processor must comply with Part III of the Policy together with the practical procedures set out in the appendices in Part IV of the Policy.
- Some Affiliates may act as both a controller and a processor and must therefore comply with Parts II, III and IV of the Policy as appropriate.

This Policy applies to all employees of Affiliates through their employment agreements and/or Helix's corporate policies. Violations may result in disciplinary action, up to and including termination of employment. As for contractors and/or contingent workers, this Policy is expressly referred to in their service agreement and violation of this Policy can lead to termination of such service agreement.

Any questions regarding the Policy can be raised with Helix's Group Data Protection Officer, responsible for monitoring compliance with the Policy.

PART II: HELIX AS A CONTROLLER

RULE 1 – COMPLIANCE WITH LOCAL LAW AND ACCOUNTABILITY

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

As an organization, Helix will comply with any applicable legislation relating to Personal Information and will ensure that where Personal Information is collected and used, this is done in accordance with the local law.

Where there is no law or the law does not meet the standards set by the Policy, Helix's position will be to process Personal Information adhering to the Policy.

To the extent that any applicable data protection legislation requires a higher level of protection, Helix acknowledges that such applicable data protection legislation will take precedence over Part II of the Policy.

Rule 1B – Helix will demonstrate its compliance with the Policy (“Accountability”)

Helix will maintain a record of processing activities carried out under its responsibility in accordance with applicable law. This record shall be maintained in writing, including in an electronic form, and shall be made available to the Competent Supervisory Authority upon request.

The record shall contain:

- the name and contact details of the Affiliate acting as the controller and, where applicable, the joint controller, and the data protection officer.
- the purposes of the processing.
- a description of the categories of individuals and of the categories of Personal Information.
- the categories of recipients to whom Personal Information has been or will be disclosed including recipients in third countries or international organizations.
- where applicable, transfers of Personal Information to a third country or an international organization, including the identification of that third country or international organization.
- where possible, the envisaged time limits for erasure of the different categories of Personal Information.
- where possible, a general description of the technical and organizational security measures applicable to processing.

In order to enhance compliance and where required, data protection impact assessments shall be carried out

for processing operations that are likely to result in a high risk to the rights and freedoms of natural persons. Where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by Helix to mitigate the risk, Helix shall consult the Competent Supervisory Authority, prior to processing.

Appropriate technical and organizational measures will be implemented which are designed to make data protection principles effective and to facilitate compliance with the requirements set out by this Policy in practice, taking into account the state of the art, cost of implementation, risks to data subjects, nature, scope, context and purpose of the processing (data protection by design and by default).

Helix will identify and implement such data protection principles when developing new IT systems, services, policies and processes that involve processing Personal Information, based on privacy by design and by default checklists.

RULE 2 – ENSURING TRANSPARENCY, FAIRNESS, PURPOSE LIMITATION, AND LAWFULNESS

Rule 2A – Helix will explain to individuals how that information will be used (“Transparency and fairness”).

Helix will ensure that individuals are told in a clear and comprehensive way (usually by means of an easily accessible fair processing statement) how their Personal Information will be used. The information Helix has to provide to individuals includes all information necessary in the circumstances to ensure that the processing of Personal Information is fair and transparent, and includes the following:

- the identity and contact details of the Helix Affiliate acting as a controller.
- the contact details of the Group Data Protection Officer.
- the purposes for which Personal Information will be processed.
- the legal basis for processing that data.
- who Personal Information will be shared with.
- countries outside of Europe where Personal Information may be transferred to, and the safeguards in place to protect it.
- the retention period for Personal Information.

- the individual rights guaranteed by Helix to request access to and rectification or erasure of Personal Information or restriction of processing or to object to processing as well as the right to data portability and the right to withdraw consent as the case may be.
- the right to lodge a complaint with a Supervisory Authority.
- the existence of automated decision-making, including profiling, and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the individual.
- whether the provision of Personal Information is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether individuals are obliged to provide Personal Information and of the possible consequences of failure to provide such information.
- the categories of Personal Information processed.

Helix will provide such information to the individual at the time when Personal Information is obtained by Helix, or at any other time specified by applicable law, unless there is a legitimate basis for not doing so (for example, where it is necessary to safeguard national security or defense, for the prevention or detection of crime, legal proceedings, or where otherwise permitted by law) or unless the individual already has such information.

Rule 2B – Helix will only obtain and use Personal Information for those purposes which are known to the individual or which are compatible with such purposes (“Purpose limitation”).

Rule 1A provides that Helix will comply with any applicable legislation relating to the collection of Personal Information. This means that where Helix collects Personal Information in Europe and local law requires that Helix may only collect and use it for specific, explicit and legitimate purposes, and not use that Personal Information in a way which is incompatible with those purposes, Helix will honor these obligations.

Under Rule 2B, Helix will identify and make known the purposes for which Personal Information will be used (including the secondary uses and disclosures of the information), prior to such processing, unless there is a legitimate basis for not doing so, as described in Rule 2A.

In particular, if Helix collects Personal Information for a specific purpose and subsequently Helix wishes to use the information for a different or new purpose, the relevant individuals will be made aware of such a change prior to that further processing unless:

- it is compatible with the initial purposes agreed with the individual; or

- there is a legitimate basis for not doing so consistent with the applicable law of the European country in which Personal Information was collected.

In certain cases, for example, where the processing is of sensitive Personal Information, or where Helix is not satisfied that the processing is compatible with the initial purposes agreed with the individual, the individual's consent to the new uses or disclosures may be necessary.

Rule 2C – Helix will process Personal Information lawfully (“Lawfulness”)

Any processing of Personal Information by Helix shall be based on one of the following legal grounds:

- (a) the individual has given consent to the processing of his Personal Information for one or more specific purposes; or
- (b) processing is necessary for the performance of a contract to which the individual is party or in order to take steps at the request of the individual prior to entering into a contract; or
- (c) processing is necessary for compliance with a legal obligation to which Helix is subject; or
- (d) processing is necessary for the purposes of the legitimate interests pursued by Helix or by a third party, where such interests are not overridden by the interests or fundamental rights and freedoms of the individuals; or
- (e) any other legal ground provided by applicable Union or Member State law.

RULE 3 – ENSURING DATA QUALITY

Rule 3A – Helix will keep Personal Information accurate and up to date (“Accuracy”).

In order to ensure that Personal Information held by Helix is accurate and up to date, Helix actively encourages individuals to inform Helix when their Personal Information changes.

Rule 3B – Helix will only keep Personal Information for as long as is necessary for the purposes for which it is collected and further processed (“Storage limitation”).

Helix will comply with Helix's record retention policies and procedures as revised and updated from time to time.

Rule 3C – Helix will only process Personal Information that is adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed (“Data minimization”).

Helix will identify the minimum amount of Personal Information necessary in order to properly fulfill its

purposes.

RULE 4 – TAKING APPROPRIATE SECURITY MEASURES AND NOTIFYING DATA BREACHES

Rule 4A – Helix will adhere to its security and breach notification policies.

Helix will implement appropriate technical and organizational measures to protect Personal Information against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Information, in particular where processing involves transmission of Personal Information over a network, and against all other unlawful forms of processing.

To this end, Helix will comply with the requirements in the security policies in place within Helix as revised and updated from time to time together with any other security procedures relevant to a business area or function.

Helix will implement and comply with breach notification policies as required by applicable data protection law:

- **Notification between Affiliates:** any Affiliate becoming aware of a Personal Information breach shall without undue delay notify the Group Data Protection Officer.
- **Notification to a Supervisory Authority:** Helix shall without undue delay and, where feasible, no later than 72 hours after having become aware of it, notify the Personal Information breach to the Competent Supervisory Authority, unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the Supervisory Authority is not made within 72 hours, it shall be accompanied by reasons for the delay.
- **Notification to individuals:** When the breach is likely to result in a high risk to the rights and freedoms of the individuals, Helix shall communicate the breach to such individuals without undue delay.

Personal Information breaches shall be documented in accordance with applicable law (including the facts relating to the breach, its consequences and the remedial action taken). Such documentation will be made available to the Competent Supervisory Authority upon request.

Rule 4B – Helix will ensure that service providers to Helix also adopt appropriate and equivalent security measures.

European law expressly requires that where service providers (acting as a processor) to any of the Helix entities have access to Personal Information of past, current and potential employees, (including contractors

and contingent workers), customers, resellers, suppliers, service providers and other third parties, strict contractual obligations evidenced in writing dealing with the security of that information are imposed consistent with the applicable law of the European country in which Personal Information was collected, to ensure that such service providers act only on Helix's instructions when using that information (unless such service provider is required to do so by applicable law), and that they have in place appropriate technical and organizational security measures to safeguard Personal Information. Whenever the service provider is not an Affiliate, Helix will make its best efforts to ensure that such service provider has committed in writing to comply with obligations consistent with this Policy.

Contracts with such service providers will set out the subject matter and duration of the processing, the nature and purpose of the processing, the type of Personal Information and categories of individuals and the obligations and rights of Helix. Such contracts shall stipulate, in particular, that the provider:

- processes Personal Information only on documented instructions from Helix, including with regard to transfers of Personal Information to a third country or an international organization, unless required to do so by Union or Member State law to which the provider is subject; in such a case, the service provider shall inform Helix of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;
- ensures that persons authorized to process Personal Information have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
- taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of individuals, implements appropriate technical and organizational measures to ensure a level of security appropriate to the risk.
- shall not engage another processor without prior specific or general written authorization of Helix. In the case of general written authorization, the service provider shall inform Helix of any intended changes concerning the addition or replacement of other processors, thereby giving Helix the opportunity to object to such changes. Where a service provider engages another processor for carrying out specific processing activities on behalf of Helix, the same data protection obligations as set out in the contract or other legal act between Helix and the service provider shall be imposed on that other processor by way of a contract or other legal act under Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organizational measures. Whereas that other processor fails to fulfil its data protection obligations, the service provider shall remain fully liable to Helix for the performance of that other processor's obligations.

- taking into account the nature of the processing, assists Helix by appropriate technical and organizational measures, insofar this is possible, for the fulfilment of Helix's obligation to respond to requests for exercising the data subject's rights laid down in GDPR.
- assists Helix in ensuring compliance with its obligations to ensure security of processing, notify Personal Information breaches, carry out data protection assessments and consult the supervisory authority, taking into account the nature of processing and the information available to the processor.
- at the choice of Helix, deletes or returns all Personal Information to Helix after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of Personal Information.
- makes available to Helix all information necessary to demonstrate compliance with the obligations laid down in GDPR and allow for and contribute to audits, including inspections, conducted by Helix or another auditor mandated by Helix. The provider shall immediately inform Helix if, in its opinion, an instruction infringes GDPR or other Union or Member State data protection provisions.

RULE 5 – HONORING INDIVIDUALS' RIGHTS

Rule 5A – Helix will adhere to the Individuals' Rights Requests Procedure and respond to any queries or requests made by individuals in connection with their Personal Information, in accordance with applicable law.

Individuals are entitled (by making a written request to Helix where required) to obtain from Helix confirmation as to whether or not their Personal Information is being processed and, where that is the case, be supplied with a copy of Personal Information held about them (including information held in both electronic and paper records). This is known as the "right of access" in European data protection law. Helix will follow the steps set out in the Individuals' Rights Requests Procedure (see Appendix 1) when dealing with requests from individuals for access to their Personal Information.

Rule 5B – Helix will deal with individual rights in accordance with the Individuals' Rights Requests Procedure.

Individuals are entitled, in accordance with applicable law, to request rectification, or erasure of their Personal Information and, in certain circumstances, to object to or restrict the processing of their Personal Information. Individuals may also exercise their right to portability. Any rectification or erasure of Personal Information or restriction of processing requested by an individual will be communicated to recipients to whom Personal Information has been disclosed, unless it proves impossible or involves disproportionate effort. Helix will inform that individual about such recipients upon request. Helix will follow the steps set out in the Individuals'

Rights Requests Procedure (see Appendix 1) in such circumstances.

Rule 5C – Where decisions regarding individuals are made solely by automated means, individuals will have the right to know the existence of the automated decision-making process and the logic involved in the decision. Helix will take necessary measures to protect the rights, freedoms and 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 produces legal effects concerning him or her, or significantly affects him or her, can be based solely on the automated processing of Personal Information, unless there is a legal basis for such decision, and measures are taken to protect the rights, freedoms and legitimate interests of individuals.

Individuals shall at least have the right to obtain human intervention on the part of Helix, to express their point of view and to contest the decision. Helix will follow the steps set out in the Individuals' Rights Requests Procedure (see Appendix 1) in such circumstances.

Rule 5D – Helix will allow customers to opt out of receiving marketing information.

All individuals have the data protection right to object, at any time and free of charge, to the use of their Personal Information for direct marketing purposes, including profiling to the extent that it is related to such direct marketing, and Helix will honor all such opt out requests and no longer process Personal Information for this purpose. Helix will follow the steps set out in the Individuals' Rights Requests Procedure (see Appendix 1) in such circumstances.

RULE 6 – ENSURING ADEQUATE PROTECTION FOR TRANSFERS OF PERSONAL INFORMATION OUTSIDE EUROPE

Rule 6 – Helix will not transfer Personal Information to third parties outside Europe without ensuring adequate protection for the information in accordance with the standards set out by the Policy.

Helix must comply with any restrictions under applicable data protection laws which prohibit the transfers of Personal Information to third countries unless appropriate steps are taken to ensure the transferred data continues to remain protected to the standard required in the country or region from which it is transferred.

Whenever Helix transfers Personal Information outside Europe, Helix must implement appropriate safeguards, such as contractual clauses so as to guarantee the level of protection of Personal Information that is being transferred outside Europe.

Helix will take appropriate action in case national legislation in a third country outside Europe prevents

compliance with this Policy.

RULE 7 – SAFEGUARDING THE USE OF SENSITIVE PERSONAL INFORMATION

Rule 7A – Helix will only transfer and use sensitive Personal Information if it is absolutely necessary.

Sensitive Personal Information is information relating to an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health data, sex life, sexual orientation, criminal convictions and offenses. Helix will assess whether sensitive Personal Information is required for the proposed use and whether it is absolutely necessary in the context of its business.

Rule 7B – Helix will only transfer and use sensitive Personal Information collected in Europe where the individual's explicit consent has been obtained unless Helix has an alternative legitimate basis for doing so consistent with the applicable law of the European country in which Personal Information was collected.

In principle, individuals must explicitly agree to Helix collecting and using sensitive Personal Information. This permission to use sensitive Personal Information by Helix must be genuine and freely given. Helix may also use sensitive Personal Information if it is required by local law or Helix has another legitimate basis for doing so, consistent with the applicable law of the country in which Personal Information was collected.

RULE 8 – COMPLIANCE

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

Helix has appointed a Group Data Protection Officer who is part of the Privacy Office to oversee and ensure compliance with the Policy. The Privacy Office is supported by legal and compliance officers at regional and country level who are responsible for overseeing and enabling compliance with the Policy on a day-to-day basis.

RULE 9 – TRAINING

Rule 9 – Helix will provide appropriate training to employees 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.

RULE 10 – AUDIT

Rule 10 – Helix will comply with the Privacy Compliance Framework Policy Audit Protocol set out in

Appendix 4.

RULE 11 – COMPLAINT HANDLING

Rule 11 – Helix will comply with the Privacy Compliance Framework Policy Complaint Handling Procedure set out in Appendix 5.

RULE 12 – COOPERATION WITH SUPERVISORY AUTHORITIES

Rule 12 – Helix will comply with the Privacy Compliance Framework Policy Cooperation Procedure set out in Appendix 6.

RULE 13 – ACTION WHERE NATIONAL LEGISLATION PREVENTS COMPLIANCE WITH THE POLICY

Rule 13A – Helix will take appropriate action if it believes that the legislation applicable to it prevents it from fulfilling its obligations under Part II of this Policy or such legislation has a substantial effect on its ability to comply with Part II of this Policy.

1. Assessment

Helix must assess, in light of all of the circumstances of a transfer, if the laws and practices in a third country outside Europe that has not been recognized by the European Commission as ensuring an adequate level of protection, applicable to the processing of Personal Information under Part II of this Policy, may impinge on the effectiveness of this Policy and thus prevent Helix from fulfilling its obligations under Part II of this Policy or has a substantial effect on the guarantees provided by this Policy.

Helix's assessment will be based on the understanding that any laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) GDPR, are not in contradiction with this Policy.

Such assessment will take due account of:

- a. the specific circumstances of the transfer, including the location of the processing, the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred Personal Information; the economic sector in which the transfer occurs; the storage location of the information transferred;
- b. the laws and practices of the third country relevant in light of the specific circumstances of the transfer, including those requiring the disclosure of information to public authorities or authorizing access by such

authorities, and those providing for access to these data during the transit between the country of the data exporter and the country of the data importer, as well as the applicable limitations and safeguards;

- c. any relevant contractual, technical or organizational safeguards put in place to supplement the safeguards under this Policy, including measures applied during transmission and to the processing of Personal Information in the third country. Helix's Group Data Protection Officer shall be informed and involved in the identification of such contractual, technical or organizational safeguards.

Helix will monitor, on an ongoing basis, developments in laws and practices of the third country that could affect the initial assessment and the decisions taken accordingly.

Helix will document the assessment and make it available to the Competent Supervisory Authority on request.

For the avoidance of doubt, this section 1 also pertains to onward transfers of Personal Information to controllers and processors that are not Affiliates.

2. Notification

If the Affiliate acting as the data importer has reasons to believe that it is or has become subject to laws or practices not in line with the requirements under Part II of this Policy, including following a change in the laws of a third country or a measure indicating an application of such laws in practice that is not in line with the requirements in Part II of this Policy, Helix will promptly inform:

- (a) The Affiliate in Europe acting as the data exporter.
- (b) Helix's Group Data Protection Officer.

except where prohibited by a law enforcement authority, such as prohibition under criminal law to preserve the confidentiality of a law enforcement investigation.

3. Supplementary measures

Following a notification pursuant to section 2, or if the Affiliate acting as the data importer, and/or the Affiliate acting as the data exporter, otherwise have reason to believe that the Affiliate acting as the data importer can no longer fulfil its obligations under Part II of this Policy, the Affiliate acting as the data exporter and the Affiliate acting as the data importer shall promptly identify supplementary measures (such as technical or organizational measures to ensure security and confidentiality) to be adopted to address the situation. Helix's Group Data Protection Officer shall be informed and involved in the identification of such supplementary measures.

The Affiliate acting as the data importer and Helix's Group Data Protection Officer will inform all other Affiliates of the assessment carried out and of its results, so that the identified supplementary measures will be applied in case the same type of transfers is carried out by any other Affiliate or, where effective supplementary measures could not be put in place, the transfers at stake are suspended or ended.

Helix will document the identification of supplementary measures and make it available to the Competent Supervisory Authority on request.

4. Suspension, return and deletion

If they consider that no appropriate supplementary measures can be ensured or if instructed by the Competent Supervisory Authority to do so, the Affiliate in Europe acting as the data exporter shall suspend the transfer of Personal Information. Such suspension shall also apply to all transfers for which the same assessment and reasoning would lead to a similar result, until compliance is again ensured or the transfer is ended. Unless compliance with the Policy is restored within one month of suspension, Personal Information that has been transferred prior to the suspension shall at the choice of the Affiliate in Europe acting as the data exporter be returned to that Affiliate or deleted in its entirety. The same shall apply to any copies of the information. The Affiliate acting as the data importer shall certify the deletion of the information to the Affiliate in Europe acting as the data exporter. Until the information is deleted or returned, the Affiliate acting as the data importer shall continue to ensure compliance with Part II of this Policy. In case of local laws applicable to the Affiliate acting as the data importer that prohibit the return or deletion of the transferred Personal Information, the Affiliate acting as the data importer warrants that it will continue to ensure compliance with Part II of this Policy and will only process the information, to the extent and for as long as required under that local law.

Rule 13B – Helix will take appropriate action if (i) it receives a legally binding request for the disclosure of Personal Information transferred pursuant to Part II of this Policy from a public authority (e.g. a law enforcement authority or state security body), including judicial authorities under the laws of a third country not recognized by the European Commission as ensuring an adequate level of protection (“Request for Disclosure”) or (ii) becomes aware of any direct access by public authorities to Personal Information transferred pursuant to this Policy in accordance with the laws of a third country.

1. Notification

If Helix receives a Request for Disclosure or becomes aware of direct access to Personal Information by a public authority in a third country, it will promptly notify:

- (a) The Affiliate in Europe acting as the data exporter.

- (b) Helix's Group Data Protection Officer.
- (c) Where possible, the individuals concerned.

Such notification shall include information about Personal Information requested, the requesting authority, the legal basis for the Request and the response provided, unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation.

If Helix is prohibited from notifying the Affiliate in Europe acting as the data exporter and/or the individuals concerned, and/or prohibited from informing the Competent Supervisory Authority, under the laws of the third country not recognized by the European Commission as ensuring an adequate level of protection, Helix will use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. Helix will document its best efforts in order to be able to demonstrate them upon request of the Affiliate acting as the data exporter.

If, despite having used its best efforts, Helix is not in a position to obtain a waiver of the prohibition, Helix will annually provide general information on the Requests it received to the Affiliate in Europe acting as the data exporter and to the Competent Supervisory Authority (e.g. number of Requests, type of data requested, requesting authorities, whether Requests have been challenged and the outcome of such challenges if possible, etc.), to the extent that Helix has been authorized by the requesting authority to disclose such information. If Helix is or becomes partially or completely prohibited from providing the Affiliate in Europe acting as the data exporter with the aforementioned information, it will, without undue delay, inform the Affiliate in Europe acting as the data exporter accordingly.

Helix will preserve the abovementioned information for as long as Personal Information is subject to the safeguards provided by this Policy and will make it available to the Competent Supervisory Authority upon request.

In no event shall Helix transfer Personal Information to any public authority in a third country in a massive, disproportionate and indiscriminate manner that goes beyond what is necessary in a democratic society.

Any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring Helix to transfer or disclose Personal Information may only be recognized or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or an EU Member State, without prejudice to other grounds for transfer pursuant to GDPR.

2. Review of legality and minimization

Helix will review the legality of the Request for Disclosure and will challenge it if, after careful assessment, it

concludes that there are reasonable grounds to consider that the Request for Disclosure is unlawful under the laws of third countries not recognized by the European Commission as ensuring an adequate level of protection, applicable obligations under international law and principles of international comity.

Helix will, under the same conditions, pursue possibilities of appeal. When challenging a Request for Disclosure, Helix will seek interim measures with a view to suspending the effects of the Request until the competent judicial authority has decided on its merits. Helix shall not disclose the Personal Information requested until required to do so under the applicable procedural rules.

Helix will document its legal assessment and any challenge to the Request for Disclosure and, to the extent permissible under the laws of the third countries not recognized by the European Commission as ensuring an adequate level of protection, make the documentation available to the Affiliate established in Europe. Helix shall make the same documentation available to the Competent Supervisory Authority on request.

Helix will provide the minimum amount of information permissible when responding to a Request for Disclosure, based on a reasonable interpretation of the Request.

RULE 14 – NON-COMPLIANCE AND TERMINATION

Rule 14A – Helix will take appropriate action if an Affiliate acting as an importer is in breach of this Policy or unable to comply with this Policy.

Helix will not transfer Personal Information to an Affiliate acting as an importer under this Policy, unless that Affiliate can deliver compliance.

The Affiliate acting as an importer will promptly inform the Affiliate acting as an exporter if it is unable to comply with this Policy, for whatever reason, including the situations further described under Rule 13 above.

In case an Affiliate acting as an importer is in breach of the Policy or unable to comply with it, the Affiliate acting as an exporter will suspend the transfer of Personal Information.

The Affiliate acting as an importer will, at the choice of the Affiliate acting as an exporter, immediately return or delete Personal Information that has been transferred under the Policy in its entirety, where:

- (i) the Affiliate acting as an exporter has suspended the transfer, and compliance with this Policy is not restored within a reasonable time, and in any event within one month of suspension; or
- (ii) the Affiliate acting as an importer is in substantial or persistent breach of this Policy; or
- (iii) the Affiliate acting as an importer fails to comply with a binding decision of a competent court or Competent Supervisory Authority regarding its obligations under the Policy.

The same commitments will apply to any copies of Personal Information transferred under this Policy. The Affiliate acting as an importer will certify the deletion of Personal Information to the Affiliate acting as an exporter.

Until Personal Information is deleted or returned, the Affiliate acting as an importer will continue to ensure compliance with this Policy. In case of local laws applicable to the Affiliate acting as an importer prohibiting the return or deletion of the transferred Personal Information, the Affiliate acting as an importer will continue to ensure compliance with the Policy, and will only process the data to the extent and for as long as required under that local law.

Rule 14B – In case an Affiliate acting as an importer ceases to be bound by the Policy, that Affiliate will keep, return, or delete Personal Information it received under Part II of this Policy.

In case an Affiliate acting as an importer ceases to be bound by the Policy, the Affiliate acting as an exporter and the Affiliate acting as an importer will determine if Personal Information transferred under the Policy will be kept, returned or deleted.

If the Affiliate acting as an exporter and the Affiliate acting as an importer agree that Personal Information must be kept by the Affiliate acting as an importer, protection must be maintained in accordance with Chapter V GDPR.

PART III: HELIX AS A PROCESSOR

Part III of this Policy applies in all cases where Helix collects, uses and transfers Personal Information as a processor on behalf of a third party under a contract evidenced in writing, in a situation where the third party will be a controller (referred to as the "Client" or "Controllers" in Part III of this Policy). The principal areas in which Helix acts as a processor include the provision of software as a service.

When Helix acts as a processor, the controller retains the responsibility to comply with European data protection law. Certain data protection obligations are passed to Helix in the contracts Helix has with its Clients, in accordance with applicable law. If Helix fails to comply with such data protection obligations, Helix may face a civil claim for breach of contract which may result in the payment of compensation or other judicial remedies, as well as an administrative sanction for a breach of applicable data protection law. If a Client demonstrates that it has suffered damage, and that it is likely that the damage occurred because of a breach of Part III of the Policy (or any of the commitments in the Introduction to the Policy or the appendices in Part IV of the Policy (as applicable)) by an Affiliate outside Europe or a third party sub-processor established outside Europe, that Client is entitled to enforce this Policy against Helix. In such cases, the obligation will be on the Affiliate accepting liability (namely the Affiliate which is a party to a contract with the Client) to show that an Affiliate outside Europe (or a third-party sub-processor established outside Europe) is not responsible for the breach, or that no such breach took place.

RULE 1 – COMPLIANCE WITH LOCAL LAW AND ACCOUNTABILITY

Rule 1A – Helix will ensure that compliance with Part III of the Policy will not conflict with applicable data protection laws where they exist.

To the extent that any applicable data protection legislation requires a higher level of protection, Helix acknowledges that it will take precedence over Part III of the Policy.

Rule 1B – Helix will cooperate and assist its Clients to comply with its obligations under data protection law in a reasonable time and to the extent reasonably possible.

Helix will, within a reasonable time, to the extent reasonably possible and according to the terms agreed in its contracts with its Clients, assist its Clients to comply with their obligations as controllers under applicable data protection law. This may include, for example, cooperating and assisting its Clients to respect the individuals' rights or to handle their complaints, or being in a position to reply to investigation or inquiry from Supervisory Authorities.

Rule 1C – Helix will make available to its Clients all information necessary to demonstrate compliance with Helix’s obligations under Part III of the Policy.

Helix will maintain a written record of the processing activities carried out on behalf of its Clients, in line with the requirements set out in applicable law and which may be made available to Supervisory Authorities upon their request.

The record shall contain:

- the name and contact details of the Affiliate acting as the processor or processors and of each Client on behalf of which the Affiliate is acting, and, where applicable, of the Client’s representative, and the data protection officer.
 - the categories of processing carried out on behalf of each Client.
 - where applicable, transfers of Personal Information to a third country or an international organization, including the identification of that third country or international organization.
 - where possible, a general description of the technical and organizational security measures applicable to processing.

Helix will make available to its Clients all information necessary to demonstrate compliance with its obligations under applicable law, and will allow for and contribute to audits, including inspections conducted by the Client, in accordance with the terms of the contract with such Client.

RULE 2 – ENSURING TRANSPARENCY, FAIRNESS, LAWFULNESS AND PURPOSE LIMITATION

Rule 2A – Helix will assist its Clients in ensuring transparency, fairness and lawfulness.

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 and this is usually done by means of an easily accessible fair processing statement. In addition, Clients must ensure that Personal Information is processed lawfully and fairly.

Helix will assist its Clients in complying with such requirements, within the limits of applicable law and as per the terms of its contracts with its Clients. For example, Helix may be required by applicable law to provide information about any sub-processors appointed by Helix to process Client Personal Information on its behalf, in which case the terms of such communication shall be detailed in the contract with that particular Client.

Rule 2B – Helix will only use Personal Information on behalf of and in accordance with the specific instructions of its Clients (“Purpose limitation”).

Helix will only use Personal Information in compliance with the terms of a contract it has with its Client, unless otherwise required by European Union or the Member State law applicable to Helix.

In such a case, Helix shall inform the Client of that legal requirement before processing takes place, unless that law prohibits such information from being disclosed on important grounds of public interest.

If, for any reason, Helix is unable to comply with this Rule or its obligations under Part III of the Policy in respect of any contract it may have with a Client, Helix will inform that Client promptly of this fact. Helix's Client may then suspend the transfer of Personal Information to Helix and/or terminate the contract, depending upon the terms of its contract with Helix.

On the termination of the provision of services to a Client, Helix will, at the choice of the Client, delete or return all Personal Information to the Client and delete the copies thereof, as required in accordance with the terms of its contract with that Client, unless European Union or Member State law requires storage of Personal Information by Helix. In that case, Helix will maintain the confidentiality of Personal Information and will no longer actively process that Personal Information, i.e., for the purposes for which it was initially collected.

RULE 3 – DATA QUALITY AND PROPORTIONALITY

Rule 3 – Helix and its sub-processors will assist its Clients to keep Personal Information accurate and up to date.

Helix will comply with any instructions from a Client, as required by applicable law and under the terms of its contract with that Client, 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 a Client, as required under the terms of its contract with that Client, Helix and its sub-processors to whom Personal Information has been provided, will delete, anonymize, update or correct Personal Information, or cease or restrict processing of Personal Information.

Helix will notify other Affiliates or any third party sub-processor to whom Personal Information has been disclosed accordingly so that they can also update their records.

RULE 4 – RESPECTING INDIVIDUALS' RIGHTS

Rule 4 – Helix will assist its Clients to comply with the rights of individuals.

Helix will act in accordance with the instructions of a Client as required under the terms of its contract with that Client and undertake any appropriate technical and organizational measures to enable its Clients to comply with their duty to

respect the rights of individuals. In particular, if Helix receives an individual's rights request, it will transfer such request promptly to the relevant Client and not respond to such a request unless authorized to do so or required by law.

RULE 5 – SECURITY AND CONFIDENTIALITY

Rule 5A – Helix will put in place appropriate technical and organizational measures to safeguard Personal Information processed on behalf of its Clients to ensure a level of security appropriate to the risk.

European law expressly requires that where Helix provides a service to a Client which involves the processing of Personal Information, the contract between Helix and its Client details the security and organizational measures required to safeguard that information in a manner appropriate with the associated level of risk and consistent with the law of the European country from which Personal Information was transferred.

Rule 5B – Helix will notify its Clients of any Personal Information breach in accordance with the terms of the contract with the Client.

Helix will notify a Client of any Personal Information breach in relation to Personal Information processed on behalf of that Client without undue delay and as required to do so under the terms of the contract with that Client. Furthermore, any Personal Information breach shall be documented in accordance with applicable law (including the facts relating to the breach, its consequences and the remedial action taken). Such documentation will be made available to the Supervisory Authority upon request of the Client, and as per the terms of the contract with such Client.

Rule 5C – Helix will comply with the requirements of its Clients regarding the appointment of any sub-processor.

Helix will inform its Clients where processing undertaken on their behalf will be conducted by a sub-processor, whether such sub-processor is an Affiliate or an external service provider, and will comply with the particular requirements of a Client with regard to the appointment of sub-processors as set out under the terms of its contract with that Client. Helix will ensure that up to date information regarding its appointment of sub-processors is available to those Clients at all times and has obtained their general written consent for such sub-processing. If a Client objects to the appointment of a sub-processor to process Personal Information on its behalf, that Client will be entitled to require from Helix that the transfer of Personal Information be suspended and/or to terminate the contract, depending on the terms of its contract with Helix.

Rule 5D – Helix will ensure that sub-processors undertake to comply with provisions which are consistent with (i) the terms of its contracts with its Clients and (ii) Part III of the Policy, and in particular that the sub-processor will adopt appropriate and equivalent technical and organizational measures.

Helix must only appoint sub-processors who provide sufficient guarantees in respect of the commitments made by Helix in Part III of the Policy. In particular, such sub-processors must be able to provide appropriate technical and organizational measures that will govern their use of Personal Information to which they will have access in accordance with the terms of the contract between Helix and a Client.

To comply with this Rule, where a sub-processor has access to Personal Information processed on behalf of Helix, Helix will take steps to ensure that it has in place appropriate technical and organizational security measures to safeguard Personal Information in accordance with applicable law 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 Part III of the Policy (and in particular Rules 5A and 5B above) and with the terms of the contract Helix has with a Client in respect of the processing in question.
- that the sub-processor will act only on Helix's instructions when using that information including with regard to transfers of Personal Information to a third country or an organization outside Europe.
- that the sub-processor will cooperate with the Supervisory Authorities and the Client in a similar way as Helix as detailed in part III of the Policy.
- such obligations as may be necessary to ensure that the commitments on the part of the sub-processor reflect those made by Helix in Part III of the Policy, and which, in particular, provide for adequate safeguards with respect to the privacy and fundamental rights and freedoms of individuals in respect of transfers of Personal Information from an Affiliate in Europe to a sub-processor established outside Europe.

Contracts with sub-processors will include in particular:

- a requirement to process Personal Information based solely on Client's instructions.
- the rights and obligations of the Client.
- the scope of processing (duration, nature, purpose and the categories of Personal Information).
- an obligation for the sub-processor to:
 - implement appropriate technical and organizational measures to protect Personal Information against accidental or unlawful destruction or loss, alteration, unauthorized disclosure or access.

- provide full cooperation and assistance to Client to allow individuals to exercise their rights under this Policy.
- provide full cooperation to Client so they can demonstrate its compliance obligations – this includes the right of audit and inspection.
- make all reasonable efforts to maintain Personal Information so that it is accurate and up to date at all times.
- return or delete the data at the request of a Client, unless required to retain some or part of the data to meet other legal obligations.
- maintain adequate confidentiality arrangements and not disclose Personal Information to any person except as required or permitted by law or by any agreement between the Client and Helix or with the Client's written consent.

RULE 6 – COMPLIANCE

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

Helix has appointed a Group Data Protection Officer who leads the Privacy Office to oversee and ensure compliance with the Policy. The Privacy Office is supported by Business Unit Representatives and Country Privacy Champions who support and enable compliance with the Policy on a day-to-day basis. A summary of these roles is set out in Appendix 2.

RULE 7 – TRAINING

Rule 7 – Helix will provide appropriate training to employees 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 Requirements set out in Appendix 3.

RULE 8 – AUDIT

Rule 8 – Helix will comply with the Privacy Compliance Framework Audit Protocol set out in Appendix 4.

RULE 9 – COMPLAINTS

Rule 9 – Helix will comply with the Privacy Compliance Framework Complaint Handling Procedure set out in Appendix 5.

RULE 10 – COOPERATION WITH SUPERVISORY AUTHORITIES

Rule 10 – Helix will comply with the Privacy Compliance Framework Cooperation Procedure set out in Appendix 6.

RULE 11 – ACTION WHERE NATIONAL LEGISLATION PREVENTS COMPLIANCE WITH THE POLICY

Rule 11A – Helix will take appropriate action if it believes that the legislation applicable to it prevents it from fulfilling its obligations under Part III of the Policy or such legislation has a substantial effect on its ability to comply with the Policy.

1. Assessment

Helix must assess, in light of all of the circumstances of a transfer, if the laws and practices in a third country outside Europe that has not been recognized by the European Commission as ensuring an adequate level of protection, applicable to the processing of Personal Information under this Policy, may impinge on the effectiveness of this Policy and thus prevent Helix from fulfilling its obligations under this Policy or has a substantial effect on the guarantees provided by this Policy.

Such assessment will take due account of:

- (a) the specific circumstances of the transfer, including the location of the processing; the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred Personal Information; the economic sector in which the transfer occurs; the storage location of the information transferred;
- (b) the laws and practices of the third country relevant in light of the specific circumstances of the transfer, including those requiring the disclosure of information to public authorities or authorizing access by such authorities, and those providing for access to these data during the transit between the country of the data exporter and the country of the data importer, as well as the applicable limitations and safeguards;
- (c) any relevant contractual, technical or organizational safeguards put in place to supplement the safeguards under this Policy, including measures applied during transmission and to the processing of

Personal Information in the third country. Helix's Group Data Protection Officer shall be informed and involved in the identification of such contractual, technical or organizational safeguards.

Helix will monitor, on an ongoing basis, developments in laws and practices of the third country that could affect the initial assessment and the decisions taken accordingly.

Helix will document the assessment and make it available to the Competent Supervisory Authority on request.

For the avoidance of doubt, this section also pertains to onward transfers of Personal Information to controllers and processors that are not Affiliates.

2. Notification

If the Affiliate acting as the data importer has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Part III of this Policy, including following a change in the laws of third countries or a measure indicating an application of such laws in practice that is not in line with the requirements in Part III of this Policy, Helix will promptly inform:

- (a) the Client, as provided for by Rule 2B (unless otherwise prohibited by a law enforcement authority) and the Affiliate acting as the data exporter.
- (b) Helix's Group Data Protection Officer.

except where prohibited by a law enforcement authority, such as prohibition under criminal law to preserve the confidentiality of a law enforcement investigation.

3. Supplementary measures

Following a notification pursuant to section 2, or if the Client and/or the Affiliate acting as the data exporter otherwise have reason to believe that the Affiliate acting as the data importer can no longer fulfil its obligations under Part III of this Policy, the Client, the Affiliate acting as the data exporter and the Affiliate acting as the data importer shall promptly identify supplemental measures (such as technical or organizational measures to ensure security and confidentiality) to be adopted to address the situation.

Helix's Group Data Protection Officer shall be informed and involved in the identification of such supplementary measures.

Helix will document the identification of supplementary measures and make it available to the Competent Supervisory Authority on request.

4. Suspension, return and deletion

If the Client or the Affiliate acting as the data exporter consider that no appropriate supplementary measures can be ensured or if instructed by the Competent Supervisory Authority to do so, or if the Affiliate acting as an exporter is unable to comply with this Policy, for whatever reason, the Client or the Affiliate acting as the data exporter shall suspend the transfer of Personal Information. Such suspension shall also apply to all transfers for which the same assessment and reasoning would lead to a similar result, until compliance is again ensured or the transfer is ended. Unless compliance with the Policy is restored within one month of suspension, Personal Information that has been transferred prior to the suspension shall at the choice of the Client immediately be returned to that Client or deleted in its entirety. The same shall apply to any copies of the information. The Affiliate acting as the data importer shall certify the deletion of the information to the Client. Until the information is deleted or returned, the Affiliate acting as the data importer shall continue to ensure compliance with Part III of this Policy. In case of local laws applicable to the Affiliate acting as the data importer that prohibit the return or deletion of the transferred Personal Information, the Affiliate acting as the data importer warrants that it will continue to ensure compliance with Part III of this Policy and will only process the information, to the extent and for as long as required under that local law.

Rule 11B – Helix will take appropriate action if (i) it receives a legally binding request for the disclosure of Personal Information transferred pursuant to Part III of this Policy from a public authority (e.g. a law enforcement authority or state security body), including judicial authorities under the laws of a third country not recognized by the European Commission as ensuring an adequate level of protection (“Request for Disclosure”) or (ii) becomes aware of any direct access by public authorities to Personal Information transferred pursuant to Part III of this Policy in accordance with the laws of a third country.

1. Notification

If Helix receives a Request for Disclosure or becomes aware of direct access to Personal Information by a public authority in a third country, Helix will promptly notify:

- (a) the Client, as provided for by Rule 2B (unless otherwise prohibited by a law enforcement authority) and the Affiliate acting as an exporter.
- (b) Helix’s Group Data Protection Officer.
- (c) where possible, the individual (if necessary, with the help of the Client).

Such notification shall include information about the Personal Information requested, the requesting authority, the legal basis for the Request and the response provided, unless otherwise prohibited, such as a prohibition under criminal law

to preserve the confidentiality of a law enforcement investigation.

Helix will put the Request on hold and inform the Competent Supervisory Authority and the appropriate Supervisory Authority competent for the Client, unless prohibited from doing so by a law enforcement authority or agency.

If Helix is prohibited from notifying the Client and/or the individuals concerned, and/or prohibited from informing the competent Supervisory Authorities, under the laws of the third country not recognized by the European Commission as ensuring an adequate level of protection, Helix will use its best efforts to obtain a waiver of the prohibition. Helix will document its best efforts in order to be able to demonstrate them on request of the Client or of the Affiliate acting as the data exporter.

If, despite having used its best efforts, Helix is not in a position to obtain a waiver of the prohibition, Helix will annually provide general information on the Requests it received to the Client and to the competent Supervisory Authorities (e.g. number of Requests, type of data requested, requesting authorities, whether Requests have been challenged and the outcome of such challenges if possible, etc.), to the extent that Helix has been authorized by the requesting authority to disclose such information. If Helix is or becomes partially or completely prohibited from providing the Client or the Affiliate in Europe acting as the data exporter with the aforementioned information, it will, without undue delay, inform the Client and the Affiliate in Europe acting as the data exporter accordingly.

Helix will preserve the information pursuant to this section 1 for the duration of the service agreement with the Client and make it available to the Competent Supervisory Authority on request.

In no event shall Helix transfer Personal Information to any public authority in a third country in a massive, disproportionate and indiscriminate manner that goes beyond what is necessary in a democratic society.

2. Review of legality and minimization

Helix will review the legality of the Request for Disclosure and will challenge it if, after careful assessment, it concludes that there are reasonable grounds to consider that the Request for Disclosure is unlawful under the laws of third countries not recognized by the European Commission as ensuring an adequate level of protection, applicable obligations under international law and principles of international comity.

Helix will, under the same conditions, pursue possibilities of appeal. When challenging a Request for Disclosure, Helix will seek interim measures with a view to suspending the effects of the Request until the competent judicial authority has decided on its merits. Helix shall not disclose the Personal Information requested until required to do so under the applicable procedural rules.

Helix will document its legal assessment and any challenge to the Request for Disclosure and, to the extent permissible under the laws of the third countries not recognized by the European Commission as ensuring an adequate level of

protection, make the documentation available to the Client. Helix shall make the same documentation available to the Competent Supervisory Authority on request.

Helix will provide the minimum amount of information permissible when responding to a Request for Disclosure, based on a reasonable interpretation of the Request.

PART IV: APPENDICES

APPENDIX 1 - INDIVIDUALS' RIGHTS REQUESTS PROCEDURE

1. Introduction

- 1.1 When Helix collects, uses or transfers Personal Information for Helix's own purposes, Helix is deemed to be a *controller* of that information and is therefore primarily responsible for demonstrating compliance of processing with the requirements of applicable data protection law.
- 1.2 When Helix acts as a controller, individuals located in Europe¹ have the following rights, which will be dealt with in accordance with the terms of this Individuals' Rights Requests Procedure ("**Procedure**"):
- Right of Access.
 - Right to Rectification.
 - Right to Erasure.
 - Right to Restrict Processing.
 - Right to Data Portability.
 - Right to Object.
 - Rights in relation to automated decision making and profiling.
- 1.3 This Procedure explains how Helix deals with an individual's rights request relating to Personal Information ("**Request**").
- 1.4 Where a Request is subject to European data protection law because it is made with respect to individuals located in Europe, such Request will be dealt with by Helix in accordance with this Procedure, but where the applicable data protection law differs from this Procedure, the local data protection law will prevail.

¹ 'Europe' means the EEA and Switzerland, in this Procedure.

- 1.5 Certain data protection obligations are passed to Helix in the contracts Helix has with its Clients, and in that case, Helix must act in accordance with the instructions of its Client and undertake any reasonably necessary measures to enable the Client to comply with its duty to respect the rights of individuals. This means that if Helix receives an individual right request in its capacity as a processor for a Client, Helix must transfer such request promptly to the relevant Client and not respond to the request unless authorized by such Client to do so.
- 1.6 Helix shall inform each recipient to whom Personal Information has been disclosed of the rectification or erasure of Personal Information, or restriction of processing, unless it is impossible or disproportionate to do so. Helix shall inform the individual about such rectification, erasure or restriction, and shall inform the individual about such recipients upon request.

2. **General Process**

- 2.1 Requests must be made in writing (where required), which can include email². Requests do not have to be official or to mention data protection law.
- 2.2 Requests will be passed to the Group Data Protection Officer via privacy@helixops.ai immediately upon receipt, indicating the date on which it was received together with any other information which may assist the Group Data Protection Officer to deal with the Request.
- 2.3 The Group Data Protection Officer will make an initial assessment of the Request to decide whether it is valid and whether confirmation of identity, or any further information, is required.
- 2.4 Where Helix has reasonable doubts about the identity of an individual making the Request, Helix may ask for additional information necessary to confirm the identity of that individual be provided.
- 2.5 Helix must respond to Requests without undue delay and in any event within one month (or any shorter period as may be stipulated under local law) of receipt of the Request. That period may be extended by two further months where necessary, taking into account the complexity and number of the Requests, in which case the individual will be informed accordingly.
- 2.6 The Group Data Protection Officer will contact the individual in writing to acknowledge receipt of the Request and, if required, seek confirmation of identity or ask for further information.
- 2.7 The Group Data Protection Officer may decline the Request if one of the below exemptions applies:

² Unless the local data protection law provides that an oral request may be made, in which case Helix will document the request and provide a copy to the individual making the request before dealing with it.

(i) Where the Request was made to a European Affiliate and relates to Personal Information held by that Affiliate, and:

- The Request is manifestly unfounded or excessive; or
- The execution of the Request would adversely affect the rights and freedoms of others.

(ii) Where the Request was made to a non-European Affiliate and relates to Personal Information held by that Affiliate, and:

- The Request is manifestly unfounded or excessive; or
- The execution of the Request would adversely affect the rights and freedoms of others; or
- Personal Information does not originate from Europe, and the execution of the Request would require disproportionate effort.

2.8 The Group Data Protection Officer will assess each Request individually to determine whether any of the above-mentioned exemptions applies.

2.9 The execution of Requests will be provided free of charge. However, in case of Requests manifestly unfounded or excessive, Helix may either charge a reasonable fee or refuse to act on the Request.

2.10 All queries relating to this Procedure are to be addressed to the Group Data Protection Officer via privacy@helixops.ai or by mail to: BMC Helix, Group Data Protection Officer, Cœur Défense - Tour A, 100 Esplanade du Général de Gaulle, 92931 Paris La Défense Cedex, France.

3. **Right of Access**

3.1 Individuals are entitled to obtain:

(i) confirmation as to whether or not Personal Information relating to them is being processed and, where that is the case.

(ii) access to Personal Information processed by Helix and the following information.

- purposes of the processing.
- categories of Personal Information concerned.

- recipients or categories of recipients to whom the information is disclosed, in particular recipients located in a third country. If the third country is not recognized by the European Commission as ensuring an adequate level of protection, individuals shall have the right to be informed of the appropriate safeguards authorizing such transfers.
- envisaged period for which Personal Information will be stored, or, if not possible, the criteria used to determine that period.
- the existence of the right to request rectification or erasure of Personal Information, or restriction of processing of Personal Information, or to object to such processing.
- right to lodge a complaint with a Supervisory Authority.
- any available information as to the source of Personal Information which had not been collected from the individual.
- the existence of automated decision-making, including profiling, and, at least in those cases, meaningful information about the logic involved in any automatic processing as well as the significance and the envisaged consequences of such processing for the individual.

4. **Right to Rectification**

- 4.1 Individuals are entitled to obtain the rectification of inaccurate Personal Information concerning them without undue delay. Taking into account the purposes of the processing, individuals have the right to have incomplete Personal Information completed, including by means of a supplementary statement.

5. **Right to Erasure ('Right to be Forgotten')**

- 5.1 Individuals are entitled to obtain the erasure of Personal Information concerning them without undue delay, where:
- (i) Personal Information is no longer necessary in relation to the purposes for which it was collected or otherwise processed; or
 - (ii) the individual has withdrawn consent on which the processing was based, and there is no other legal ground for the processing; or
 - (iii) the individual has objected to the processing and there are no overriding legitimate grounds for the

processing, or the individual has objected to the processing for direct marketing purposes; or

(iv) Personal Information has been unlawfully processed; or

(v) Personal Information must be erased for compliance with a legal obligation in European or Member State law to which Helix is subject.

(vi) Personal Information has been collected in relation to the offer of information society services to children.

6. **Right to Restrict Processing**

6.1 Individuals are entitled to obtain restriction of processing, where:

(i) The accuracy of Personal Information is contested by the individual concerned, for a period enabling Helix to verify its accuracy.

(ii) The processing is unlawful and the individual opposes the erasure of Personal Information and requests restriction of their use instead.

(iii) Helix no longer needs Personal Information for the purpose of the processing, but it is required by the individual for the establishment, exercise or defense of legal claims; or

(iv) The individual has objected to processing pending the verification whether the legitimate grounds of Helix override those of the individual.

7. **Right to Data Portability**

7.1 Individuals are entitled to receive their Personal Information in a structured, commonly used and machine-readable format and to transfer it to another controller without hindrance where:

(i) Personal Information is processed based on consent or on a contract with the individual.

(ii) The processing is carried out by automated means.

8. **Right to Object**

8.1 Individuals are entitled to object, on particular grounds, to processing of their Personal Information, where Personal Information:

(i) is processed based on public interest or official authority vested in Helix, or Helix legitimate interests, unless Helix has a compelling legitimate ground for the processing which overrides the interests, rights and freedoms of the Individual or for the establishment, exercise or defense of legal claims.

(ii) is processed for direct marketing purposes, which includes profiling related to such direct marketing.

9. **Right in relation to automated decision-making and profiling**

9.1 Individuals are entitled not to be subject to a decision based on automated processing, including profiling, which produces legal effects or similarly significantly affects them, unless the decision:

(i) is necessary for entering into or performing a contract between Helix and the individual.

(ii) is authorized by applicable European law; or

(iii) is based on the individual's explicit consent.

APPENDIX 2 - COMPLIANCE STRUCTURE

Helix has implemented a compliance structure designed to ensure and oversee privacy compliance. This comprises teams dedicated to ensuring effective governance of the Privacy Compliance Framework Policy (the "**Policy**") and other privacy related policies, objectives and standards within Helix.

1. Executive Steering Committee

This committee consists of members of the Helix executive leadership having global responsibility for legal, compliance and ethics, human resources, information technology, security, business continuity management, privacy, and procurement. The role of the Executive Steering Committee is to provide senior executive governance and oversight of the Policy, including:

- (i) Ensuring that the Policy and other privacy related policies, objectives and standards are defined and communicated.
- (ii) Providing clear and visible senior management support and resources for the Policy and for privacy objectives and initiatives in general.
- (iii) Evaluating, approving and prioritizing remedial actions consistent with the requirements of the Policy, strategic plans, business objectives and regulatory requirements.
- (iv) Periodically assessing privacy initiatives, accomplishments, and resources to ensure continued effectiveness and improvement.
- (v) Ensuring that Helix's business objectives align with the Policy and related privacy and information protection strategies, policies and practices.
- (vi) Facilitating communications on the Policy and privacy topics with the Helix Executive Leadership Team and Board of Directors.
- (vii) Instigating and assisting in determining the scope of audits of compliance with the Policy, as described in Audit Protocol ("Audit Protocol").

2. Business Unit Representatives & Country Privacy Champions

Helix maintains a network of Business Unit Representatives which consists of mid-level executives and managers from all functional areas where Personal Information is processed, including human resources, legal, compliance and ethics,

internal controls and assurance, customer support, information technology, information security, sales, marketing, finance, consulting services, education services, order management, research and development, global security and Group privacy. The network of Business Representatives is complemented by Country Privacy Champions, who are designated by the Privacy Office to support this Policy at a country level.

Business Unit Representatives are responsible for:

- (i) Promoting the Policy at all levels in their organizations.
- (ii) Facilitating in-depth reviews of business processes for assessing compliance with the Policy as necessary.
- (iii) Ensuring that Helix's business objectives align with the Policy and related privacy and information protection strategies, policies and practices.
- (iv) Assisting the Privacy Office in identifying, evaluating, prioritizing, and driving remedial actions consistent with Helix's policies and regulatory requirements.
- (v) Implementing decisions made by the Executive Steering Committee within Helix on a global scale.

Country Privacy Champions are responsible for:

- (i) Supporting the Policy at country level, including by sharing relevant information and raising awareness with employees on privacy matters.
- (ii) Addressing employee privacy questions and escalating to the Privacy Office as necessary.

3. Global Privacy Office

The Global Privacy Office ('Privacy Office') has primary responsibility for ensuring that Helix complies with the Policy and with global privacy regulations on a day-to-day basis. The Privacy Office is headed by Helix's Group Data Protection Officer. Helix's Group Data Protection Officer will not have any tasks that could result in a conflict of interest and will inform Affiliates' highest management level if any questions or problems arise during the performance of his duties.

Helix's Privacy Office is responsible for monitoring compliance with the Policy and will have senior management support in fulfilling this role. In particular, Helix's Privacy Office is responsible for:

- (i) Informing and advising Affiliates on their obligations.

- (ii) Monitoring compliance by Affiliates.
- (iii) Providing advice to Affiliates as regards data protection impact assessments.
- (iv) Cooperating with Supervisory Authorities.
- (v) Acting as a contact point for Supervisory Authorities.

The role of the Privacy Office involves managing compliance with the day-to-day aspects of the Policy and Helix's privacy initiatives including:

- (i) Responding to inquiries and complaints relating to the Policy from individuals assessing the collection and use of Personal Information by Affiliates for potential privacy-related risks and identifying and implementing processes to address any areas of non-compliance.
- (ii) Working closely with appointed local privacy champions in driving the Policy and related policies and practices at the local country level, providing guidance and responding to privacy questions and issues.
- (iii) Providing input on audits of the Policy, coordinating responses to audit findings and responding to inquiries of the Supervisory Authorities.
- (iv) Monitoring changes to global privacy laws and ensuring that appropriate changes are made to the Policy and Helix's related policies and business practices.
- (v) Promoting Policy and privacy awareness across business units and functional areas through privacy communications and training.
- (vi) Evaluating privacy processes and procedures to ensure that they are sustainable and effective.
- (vii) Reporting periodically on the status of the Policy to the Executive Steering Committee.
- (viii) Hosting and coordinating meetings as necessary.
- (ix) Overseeing training for employees on the Policy and on data protection legal requirements in accordance with the requirements of the Privacy Training Requirements.
- (x) Escalating issues relating to the Policy to the Executive Steering Committee where required.

APPENDIX 3 - PRIVACY TRAINING REQUIREMENTS

1. Background

- 1.1 The Privacy Compliance Framework Policy (the "**Policy**") provides a framework for the transfer of Personal Information between Helix affiliates ("**Affiliates**"). The purpose of the Privacy Training Requirements document is to provide a summary as to how Helix trains such individuals on the requirements of the Policy.
- 1.2 Helix's Compliance Office has overall responsibility for compliance and ethics training within Helix, including the delivery of Helix's formal privacy online training modules. Training on the Policy is overseen by Helix's Privacy Office as the subject matter expert, supported by Helix's Compliance Office.
- 1.3 Employees 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 receive additional, tailored training on Policy and specific data protection issues relevant to their role. This training is further described below and is repeated on a regular basis. Similarly, employees responsible for specific areas of compliance with the Policy, such as responding to individuals' rights requests or handling complaints, receive specific training in these areas.

2. Overview of training

- 2.1 Compliance Training at Helix is carried out on a quarterly basis and covers a range of subjects, including data privacy, confidentiality and information security. Each year, one quarter's training is devoted to Helix's Code of Conduct (the "Code").
- 2.2 In addition to the quarterly training described in section 2.1, Helix also provides specific training on the Policy as described in section 4 below.

3. Aims of data protection and privacy training at Helix

- 3.1 The aim of Helix's privacy training is to ensure that:
 - 3.1.1 employees have an understanding of the basic principles of data privacy, confidentiality and information security.
 - 3.1.2 employees understand the Code.

3.1.3 employees in positions having 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, receive appropriate training, as described in section 4, to enable them to process Personal Information in accordance with the Policy.

3.2 General data protection and privacy training for new employees

3.2.1 New employees must complete Helix's Compliance training on the Code, information security, and data privacy shortly after joining Helix. The Code requires employees to follow Helix's relevant data protection and privacy policies.

3.3 General data protection and privacy training for all employees

3.3.1 Employees worldwide receive periodic training on data protection and privacy as part of the Compliance training process. This training covers basic data privacy rights and principles and data security in line with the requirements of the Policy. It is designed to be both informative and user-friendly, generating interest in the topic. Completion of the course is monitored and enforced by Helix's Compliance Office and employees must correctly answer a series of multiple-choice questions for the course to be deemed complete.

3.3.2 All employees also benefit from:

- all Compliance training modules, including data protection modules, which can be accessed online at any time.
- ad-hoc communications consisting of emails, awareness messaging placed on Helix intranet pages, and information security posters displayed in offices which convey the importance of information security and data protection issues relevant to Helix, including for example, social networking, remote working, engaging data processors and the protection of confidential information.

4. Training on the Policy

4.1 Employees receive training on the Policy appropriate to their roles and responsibilities within Helix.

4.2 New employees are trained on the Policy as part of their onboarding. Training is regularly delivered to current employees, on a biennial basis or more frequently if necessary.

4.3 Helix's training on the Policy is kept up to date and covers the following main areas:

4.3.1 Background and rationale:

- (a) What is data protection law?
- (b) How data protection law will affect Helix internationally, including procedures for managing requests for access to Personal Information by public authorities
- (c) The scope of the Policy
- (d) Terminology and concepts

4.3.2 The Policy:

- (a) An explanation of the Policy
- (b) Practical examples
- (c) The rights that the Policy gives to individuals
- (d) The data protection and privacy implications arising from the processing of Personal Information on behalf of clients

4.3.3 Where relevant to an employee's role, training will cover the following procedures under the Policy:

- (a) Individuals' Rights Requests Procedure
- (b) Audit Protocol
- (c) Cooperation Procedure
- (d) Complaint Handling Procedure
- (e) Data breach handling

5. Further information

- 5.1 Any queries about training under the Policy should be addressed to the Compliance Office which can be contacted by email at: compliance@helixops.ai.

APPENDIX 4 - AUDIT PROTOCOL

1. Background

- 1.1 The purpose of this Privacy Compliance Framework Policy (the “**Policy**”) is to safeguard Personal Information transferred between the Helix affiliates (“**Affiliates**”).
- 1.2 One of the roles of Helix’s Privacy Office is to provide guidance about the collection and use of Personal Information subject to the Policy and to assess the collection and use of Personal Information by Affiliates 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 ongoing basis.
- 1.3 This Audit Protocol describes the formal assessment process adopted by Helix to ensure compliance with the Policy, managed by Helix’s Assurance Department, as a way for Helix to ensure that the provisions of the Policy are observed and corrective actions taken as required.

2. Approach

2.1 Overview of audit

- 2.1.1 Compliance with the Policy is overseen on a day-to-day basis by the Privacy Office.
- 2.1.2 Helix’s Assurance Department (consisting of Internal Audit, Internal Controls, and IT Assurance functions) is responsible for performing and/or overseeing independent audits of compliance with the Policy and will ensure that such audits address all aspects of the Policy in accordance with the Helix audit program. Helix’s Assurance Department is responsible for ensuring that any issues or instances of non-compliance are brought to the attention of Helix’s Privacy Office and the Executive Steering Committee and that any corrective actions to ensure compliance take place within a reasonable timescale.
- 2.1.3 To the extent that Helix acts as a controller, audits of compliance with the commitments made in Part II of the Policy may also be extended to any processor acting on Helix’s behalf in respect of such processing.

2.2 Timing and scope of audit

- 2.2.1 Audit of the Policy will take place:
 - (a) annually in accordance with Helix’s corporate audit program; and/or

(b) at the request of Helix's Privacy Office or the Executive Steering Committee; and/or

(c) as determined necessary by the Assurance Department.

2.2.2 To the extent that an Affiliate processes Personal Information on behalf of a third-party controller, audit of the Policy will take place as required under the contract in place between that Affiliate and that third-party controller.

2.2.3 The scope of the audit performed will be determined independently by Helix's Assurance Department with consideration given to input received from the Privacy Office and Executive Steering Committee based on the use of a risk-based analysis which will consider relevant criteria, for example: areas of current regulatory focus; areas of specific or new risk for the business; areas with changes to the systems or processes used to safeguard information; areas where there have been previous audit findings or complaints; the period since the last review; and the nature and location of Personal Information processed.

2.2.4 In the event that a third-party controller on whose behalf Helix processes Personal Information exercises its right to audit Helix for compliance with Part III of the Policy, the scope of the audit shall be limited to the data processing facilities and activities relating to that controller. Helix will not provide a controller with access to systems which process Personal Information of other controllers.

2.3 Auditors

2.3.1 Audit of the Policy will be undertaken by Helix's Assurance Department. Helix may utilize other accredited internal or external auditors as determined by Helix. Auditors will be guaranteed independence as to the performance of their duties related to their audit mission. Auditors cannot be used if their designation may result in a conflict of interests.

2.3.2 In the event that a third-party controller on whose behalf Helix processes Personal Information exercises their right to audit Helix for compliance with Part III of the Policy, such audit may be undertaken by that controller or by independent, accredited auditors selected by that controller as stipulated in the contract between Helix and that controller.

2.3.3 The Helix Audit Committee, consisting of members of the Board of Directors of BMC Helix, Inc. (the "Board"), is appointed by the Board to assist it in fulfilling its oversight responsibilities with respect to matters including Helix's legal and regulatory compliance and the performance of internal audit functions and external auditors.

2.3.4 The Audit Committee is independent and reports regularly to the Board on its findings and recommendations, including in relation to the performance of external auditors and Helix's internal audit function.

2.4 Report

2.4.1 Helix's Assurance Department will provide the results of any audit of the Policy to Helix's Privacy Office, including Helix's Group Data Protection Officer, to the Executive Steering Committee and to other appropriate management personnel. The Assurance Department will also provide a summary of the audit results to the Audit Committee, which reports directly to the Board.

2.4.2 Helix has agreed to:

- (a) provide copies of the results of any audit of the Policy to a Supervisory Authority of competent jurisdiction upon that Authority's request.
- (b) to the extent that an audit relates to Personal Information processed by Helix on behalf of a third-party controller, to make the results of any audit of compliance with Part III of the Policy available to that controller.

APPENDIX 5 - COMPLAINT HANDLING PROCEDURE

1. Introduction

The Privacy Compliance Framework Policy (the "Policy") safeguards Personal Information processed or transferred between the Helix affiliates ("Affiliates"). The purpose of this Complaint Handling Procedure is to explain how complaints brought by an individual whose Personal Information is processed by Helix under the Policy are dealt with.

2. How individuals can bring complaints

Individuals can bring complaints in writing by contacting Helix's Group Data Protection Officer via email to privacy@helixops.ai or by mail to: BMC Helix, Group Data Protection Officer, Cœur Défense - Tour A, 100 Esplanade du Général de Gaulle, 92931 Paris La Défense Cedex, France. These are the contact details for all complaints made under the Policy and whether Helix 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 Helix is a controller

Helix's Group Data Protection Officer will handle all complaints arising under the Policy where a complaint is brought in respect of the collection and use of Personal Information where Helix is the controller of that information. Helix's Group Data Protection Officer will liaise with its colleagues from the relevant business and support units as appropriate to deal with the complaint.

Unless exceptional circumstances apply, Helix's Group Data Protection Officer will acknowledge receipt of a complaint to the individual concerned within 5 working days, investigating and making a substantive response within one month. Such response will include information on actions taken by Helix.

If, due to the complexity of the complaint or the number of received complaints, a substantive response cannot be given within this period, Helix's Group Data Protection Officer will advise the complainant accordingly and provide a reasonable estimate (not exceeding two additional months) for the timescale within which a response will be provided.

If the complainant disputes the response of the Group Data Protection Officer (or the individual or department within Helix tasked by the Group Data Protection Officer with resolving the complaint) or any aspect of a finding, and notifies the Group Data Protection Officer accordingly, the matter will be referred to Helix's General Counsel who will review the case and advise the complainant of his or her decision either to accept the original finding or to substitute a new finding. Helix's General Counsel will respond to the complainant within six months of the referral. As part of the review, Helix's

General Counsel may arrange to meet the parties in an attempt to resolve the complaint.

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

Individuals whose Personal Information is transferred under this Policy also have the right to lodge a complaint to the Competent Supervisory Authority located in the country of the individual's habitual residence, place of work or place of the alleged infringement; and/or to lodge a claim with a court of competent jurisdiction where Helix has an establishment, or where the individuals have their habitual residence. Individuals may lodge such a claim or complaint whether or not they have first made a complaint to Helix and without having exhausted this Complaint Handling Procedure beforehand.

If the matter relates to Personal Information which has been exported to an Affiliate outside Europe and an individual wants to make a claim against Helix, the claim may be made against the Affiliate acting as the data exporter.

3.2 Complaints where Helix is a processor

Where a complaint is brought in respect of the collection and use of Personal Information where Helix is the processor in respect of that information, Helix 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 Helix if the Client requires that Helix investigate the complaint.

In circumstances where a client has disappeared factually, no longer exists in law or has become insolvent, Helix will handle such complaints in accordance with section 3.1. of this Complaint Handling Procedure. In such cases, individuals also have the right to complain to the Competent Supervisory Authority and/or to lodge a claim with a court of competent jurisdiction and this includes where they are not satisfied with the way in which their complaint has been resolved by Helix. Individuals entitled to such rights will be notified accordingly as part of the Complaint Handling Procedure.

APPENDIX 6 - COOPERATION PROCEDURE

1. Introduction

This Cooperation Procedure sets out the way in which Helix will cooperate with the European³ Supervisory Authorities in relation to the Privacy Compliance Framework Policy (the "Policy").

2. Cooperation Procedure

Where required, Helix will make the necessary personnel available for dialogue with a Supervisory Authority in relation to the Policy.

On any issue related to this Policy, Affiliates will:

- a) cooperate with, and agree to be audited and inspected, including where necessary, on-site, by the competent Supervisory Authorities.
- b) take into account their advice.
- c) abide by decisions of these Supervisory Authorities

Helix agrees that:

- a) where any Helix Affiliate is located within the jurisdiction of a Supervisory Authority based in Europe, Helix agrees that this Supervisory Authority may audit that Affiliate for the purpose of reviewing compliance with the Policy, in accordance with the applicable law of the country in which the Affiliate is located.
- b) in case of an Affiliate located outside Europe, Helix agrees that a Supervisory Authority based in Europe may audit that Affiliate for the purpose of reviewing compliance with the Policy in accordance with the applicable law of the European country from which Personal Information is transferred under the Policy (which, when Helix acts as a processor on behalf of a third party controller, will be determined by the place of establishment of the controller).
- c) Any dispute related to a Competent Supervisory Authority's exercise of supervision of compliance with this Policy will be resolved by the courts of the Member State of that Supervisory Authority, in accordance with that Member State's procedural law. Affiliates agree to submit themselves to the jurisdiction of these courts.

³ For the purpose of this Policy, reference to Europe means the EEA (namely the EU Member States plus Norway Iceland and Liechtenstein) and Switzerland.

APPENDIX 7 – MATERIAL SCOPE

1. Introduction

- 1.1 This Appendix sets out the material scope of Helix's Privacy Compliance Framework Policy. It specifies a non-exhaustive list of data transfers or sets of transfers, including the nature and categories of Personal Information, the type of processing and its purposes, the types of individuals affected, and the identification of the third country or countries.

2. Material scope as a Controller

- 2.1 This section sets out the material scope of Part II of Helix's Privacy Compliance Framework.

▪ Customer relationship data (Sales & Marketing)

Who transfers the Personal Information described in this section?	Affiliates may transfer Personal Information that they control described in this section to every other Affiliate.
Who receives this Personal Information?	Every Helix Affiliate may receive Personal Information described in this section which is sent to them by another Affiliate.
What categories of Personal Information are transferred?	- Contact Information, such as address, contact telephone numbers (landline and mobile) and personal email address. - Employment information, such as job title, roles and company.
What special categories of Personal Information (if any) are transferred?	Helix does not collect or otherwise process special categories of Personal Information, as defined by Articles 9 and 10 of GDPR.
Who are the types of individuals whose Personal Information are transferred?	Sales prospects and customers.
Why is this Personal Information transferred and how will it be processed?	Sales and Marketing activities are managed both at local, regional and global levels, for purposes and in accordance with the lawful basis described below: Engage in and process transactions (Lawful basis: Helix's legitimate interest).

	Use Helix customer relationship management systems (Lawful basis: Helix's legitimate interest). Manage customers' clickwrap acceptance of Helix's license agreements (Lawful basis: Helix's legitimate interest). Review bid processes (Lawful basis: Helix's legitimate interest). Respond to inquiries and requests (Lawful basis: Helix's legitimate interest). Provide information on Helix products and services, on Helix's partners offering and Helix's services and products (Lawful basis: Helix's legitimate interest or consent as the case may be). Manage export compliance (Lawful basis: Helix's legitimate interest). Send satisfaction surveys (Lawful basis: Helix's legitimate interest). Process orders for billing, booking, accounting and invoicing purposes (Lawful basis: Helix's legitimate interest).
Where is this Personal Information processed?	Personal Information described in this section may be processed in every territory where Helix Affiliates or their processors are located.

▪ **Human Resources data**

Who transfers the Personal Information described in this section?	Affiliates may transfer Personal Information that they control described in this section to every other Affiliate.
Who receives this Personal Information?	Every Affiliate may receive Personal Information described in this section which is sent to them by another Affiliate.
What categories of Personal Information are transferred?	- Personal Identification, such as first name, second name and date of birth. - Contact Information, such as home address, contact telephone numbers (landline and mobile) and personal email address. - Education & Skills, such as employment and education history including qualifications, job application, employment references.

	- Family Information, such as emergency contacts and contact information. - Employment Information, such as job title, start and leave dates, employment contract and promotions, performance reviews and ratings, details of any leave, disciplinary records, training history and development needs. - User Account Information, such as employee ID and credentials, - Geographical Information, such as location of employment. - Financial Information, including compensation, payroll, benefits, expenses or other payments claimed and bank account details. - Government Identifiers, such as passport and national ID. - Citizenship or Immigration Status. - IT systems monitoring, such as logs. - Photos and CCTV images.
What special categories of Personal Information (if any) are transferred?	- Health information, such as accident records and health management questionnaires, to the extent authorized by applicable Member State law. Processing of health information is necessary for the purposes of carrying out the obligations and exercising specific rights in the field of employment and social security and social protection law, preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment on the basis of applicable Member State law. Such Personal Information is collected and otherwise processed in accordance with Article 6 and 9 of GDPR. Health information is subject to an obligation of secrecy under applicable Member State law. - Criminal offence information, to the extent authorized by applicable Member State law providing appropriate safeguards for the rights and freedom of individuals. Processing criminal offence information is necessary for the purpose of criminal record checks. Such Personal Information is collected and otherwise processed in accordance with Article 6 and 10 of GDPR.
Who are the types of individuals whose Personal	Applicants and employees (both current and former).

Information are transferred?	
Why is this Personal Information transferred and how will it be processed?	HR activities are managed both at local, regional and global levels, for these purposes and in accordance with the lawful basis described below: - Administer employment, including employment verifications and background checks, delivery of employment and travel letters, regulatory reporting, training, administration of lunch vouchers, internal reporting, resolution of employee requests, leave management, assistance with immigration and visa processing, new hire provisioning, candidates sourcing on social networks, performance assessments (Lawful basis: Helix's legitimate interest or performance of a contract with the individual as the case may be); - Administer compensation and benefits, including salary, bonuses, long term incentive programs, health, welfare and retirement plans (Lawful basis: Performance of a contract with the individual). - Manage payroll, including employee paychecks, benefit deductions, payroll taxes, direct deposit, garnishments/levies/child support, exception pay (bonuses, commissions, etc.), hours worked, final pay, unused PTO pay-out, leaves of absence (Lawful basis: Performance of a contract with the individual). - Administer corporate credit card program and reimburse business expenses (Lawful basis: Helix's legitimate interest). - Protect employee safety and security, including travel, office & parking access control, assistance in case of a medical emergency, CCTV (Lawful basis: Helix's legitimate interest or compliance with a legal obligation as the case may be). - Assign desks, drawers and corporate devices such as mobiles and laptops (Lawful basis: Helix's legitimate interest). - Provide IT tools and services to employees, including email and other collaboration tools (Lawful basis: Helix's legitimate interest). - Ensure secure use of IT tools and services, including identity federation, email and outbound file transfer protections, endpoint protection, cloud service monitoring, cybersecurity logging and forensics (Lawful basis: Helix's legitimate interest).

	- Monitor business mobile costs (Lawful basis: Helix's legitimate interest). - Provide company lease cars and fuel cards (Lawful basis: Helix's legitimate interest). - Make business travel arrangements (Lawful basis: Helix's legitimate interest). - Support internal and external communications, including employee communications, surveys, events and challenges (Lawful basis: Helix's legitimate interest). - Maintain Helix organizational charts (Lawful basis: Helix's legitimate interest). - Issue emergency communications and maintain business continuity in case of an emergency situation, including relocation to recovery site (Lawful basis: Helix's legitimate interest). - Perform financial planning, accounting and tax management (Lawful basis: Helix's legitimate interest). - Support the delivery of Helix products & services to customers, including use of IT tools and resources to administer, maintain and support such products & services (Lawful basis: Helix's legitimate interest). - Comply with applicable laws & regulations, including anti-discrimination, privacy, export control, and Know Your Customer ("KYC") banking requirements for company directors and bank account signers (Lawful basis: Compliance with a legal obligation). - Interact with local works councils (Lawful basis: Compliance with a legal obligation). - Monitor compliance with company policies and procedures, including training, internal controls, assessments, questionnaires, testing and Helix Integrity Helpline (Lawful basis: Helix's legitimate interest). - Protect Helix interests in contentious and non-contentious legal matters, which includes HR performance management and discipline, litigation holds, investigations, patent registration, contract negotiations, the performance of audits and compliance training (Lawful basis: Helix's legitimate interest).
--	--

	- support other business and employment-related activities (Lawful basis: Helix's legitimate interest).
Where is this Personal Information processed?	HR activities are managed both at local, regional and global levels. Personal Information described in this section may be processed in every territory where Helix Affiliates or their processors are located.

▪ **Supplier / Vendor data**

Who transfers the Personal Information described in this section?	Helix Affiliates may transfer Personal Information that they control described in this section to every other Affiliate.
Who receives this Personal Information?	Every Helix Affiliate may receive Personal Information described in this section which is sent to them by another Affiliate.
What categories of Personal Information are transferred?	Personal details. Contact details. Goods and services provided. Financial details. Employment information. Education and training details.
What special categories of Personal Information (if any) are transferred?	Helix does not collect or otherwise process special categories of Personal Information, as defined by Articles 9 and 10 of GDPR.
Who are the types of individuals whose Personal Information are transferred?	Suppliers / Vendors
Why is this Personal Information transferred and how will it be processed?	Supplier management activities are performed both at local, regional and global levels, for purposes and in accordance with the lawful basis described below: - Procurement management, including supplier selection and due diligence activities (Lawful basis: Helix legitimate interest). - Engage in and process transactions (Lawful basis: Helix's legitimate interest). - Use Helix supplier management systems (Lawful basis: Helix's legitimate interest).

	- Manage supplier acceptance of Helix's agreements (Lawful basis: Helix's legitimate interest). - Respond to inquiries and requests (Lawful basis: Helix's legitimate interest). - Manage export compliance (Lawful basis: Compliance with a legal obligation). - Process supplier orders for payment purposes (Lawful basis: Helix's legitimate interest).
Where is this Personal Information processed?	Personal Information described in this section may be processed in every territory where Helix Affiliates or their processors are located.

▪ **Business Partners / Resellers data**

Who transfers the Personal Information described in this section?	Affiliates may transfer Personal Information that they control described in this section to every other Affiliate.
Who receives this Personal Information?	Every Helix Affiliate may receive Personal Information described in this section which is sent to them by another Affiliate.
What categories of Personal Information are transferred?	Personal details, Contact details.
What special categories of Personal Information (if any) are transferred?	Helix does not collect or otherwise process special categories of Personal Information, as defined by Articles 9 and 10 of GDPR.
Who are the types of individuals whose Personal Information are transferred?	Business Partners / Resellers
Why is this Personal Information transferred and how will it be processed?	Partner management activities are performed both at local, regional and global levels, for purposes and in accordance with the lawful basis described below: - Performing sales, support, consulting services, training, research and development, and marketing activity (Lawful basis: Helix's legitimate interest or consent as the case may be).
Where is this Personal Information processed?	Personal Information described in this section may be processed in every territory where Helix Affiliates or their processors are located.

3. Material scope as a Processor

3.1 This section sets out the material scope of Part III of the Privacy Compliance Framework Policy of Helix.

▪ Customer data

Who transfers the Personal Information described in this section?	Affiliates may transfer Personal Information that they process described in this section to every other Affiliate, subject to Controller's instructions.
Who receives this Personal Information?	Every Affiliate may receive Personal Information described in this section, which is sent to them by another Affiliate, subject to Controller's instructions.
What categories of Personal Information are transferred?	The extent of Customer data processed and transferred by Helix is determined and controlled by Customer in its sole discretion. It will include Personal Information relating to the following categories of Personal Information: • Contact details, such as name, professional phone number, professional email address, professional office address, title, degree, date of birth. • Product usage data, such as media used, file type used, file size, usage and status and information related to Helix Products such as location, language, software version, data sharing choices and update details. • Connection data, such as number of times customer contact has engaged Helix Support center, duration of the engagement, means by which customer contacted Helix (by email, videoconference, Support center, etc.), region, language, time zone, localization. • Device data, such as information about Computers, and/or devices such as operating system, amount of memory, region, language, time zone, model number, first start date, age of Computer and/or device, device manufacture date, browser version, computer manufacturer, connection port, device identifiers and additional technical information that varies by Product. • Other Personal Information provided by an individual when she/he interacts, online or by phone, or mail with the Support Centers, help desks and other

	customer support channels to facilitate delivery of Helix Services and to respond to Customer or individual inquiries. Any other Personal Information Customer or Customer's Users submit, send or store via Helix Subscription Services.
What categories of sensitive Personal Information (if any) are transferred?	No sensitive Personal Information is knowingly processed by Helix.
Who are the types of individuals whose Personal Information are transferred?	- Prospects, customers, business partners and vendors of customer. - Customer's personnel, including employees, agents and contractors. - Customer's users authorized by customer to use Helix Services. No children's Personal Information is knowingly processed by Helix.
What categories of sensitive Personal Information (if any) are transferred?	No sensitive Personal Information is knowingly processed by Helix.
Who are the types of individuals whose Personal Information are transferred?	- Prospects, customers, business partners and vendors of customer. - Customer's personnel, including employees, agents and contractors. - Customer's users authorized by customer to use Helix Services. No children's Personal Information is knowingly processed by Helix.
Why is this Personal Information transferred and how will it be processed?	Helix Products and Services are delivered at local, regional and global levels, and include the provision of: - Software as a Service and cloud computing products. - outsourced helpdesk services. - customer support activity. - educational services. - analytics products. - services to members of the Helix group of companies. Helix uses a tiered support structure to ensure Customers get the best responses to their support requests as quickly as possible. Helix support is always available

	24x7x365. Helix uses a Follow the Sun approach to ensure Customers have access to Customer Support 24 hours a day through Regional Support Centers strategically placed in Asia-Pacific, Australia, Europe, Latin America, and the United States. After regular business hours of a given support location, severity one tickets are transferred to another support center located in a different time zone. Customer support activities include: - Performing detailed case analysis. - Reproducing customer problems. - Developing and providing workarounds and resolutions to customers. - Escalating issues to Level 3 support or development. - Maintaining ftp and web site content - product patches/fixes and information distribution sites. - Creating failures and requests associated with Customer cases and providing status information to the affected customers.
Where is this Personal Information processed?	Personal Information described in this section may be processed in every territory where Helix Affiliates or their processors are located.

