Personal Information Handling Procedures: Processor Policy

Contents

INTRODUCTION TO THIS POLICY

This Global Processor Personal Information Handling Policy (the "**Policy**") establishes rMark Bio, Inc. ("Company," "rMark Bio, Inc," "we," "us, "our") approach to compliance with data protection law and accordance with Privacy Shield Principles set forth in Appendix 1, and specifically to transfers of personal information between Company group members when processing that information on behalf of a third party or another business, data controller or subprocessor. rMark Bio, Inc. complies with the EU-U.S. Privacy Shield Framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information transferred from the European Union and the United Kingdom to the United States in reliance on Privacy Shield. rMark Bio has certified that it adheres to the Privacy Shield Principles with respect to such data. If there is any conflict between the policies in this privacy policy and data subject rights under the Privacy Shield Principles, the Privacy Shield Principles shall govern. To learn more about the Privacy Shield program, and to view our certification page, please visit https://www.privacyshield.gov/

rMark Bio, Inc. has further committed to refer unresolved privacy complaints under the Privacy Shield Principles to an independent dispute resolution mechanism, the BBB EU PRIVACY SHIELD. If you do not receive timely acknowledgment of your complaint, or if your complaint is not satisfactorily addressed, please visit https://bbbprograms.org/privacy-shield-complaints/ for more information and to file a complaint. This service is provided free of charge to you.

If your Privacy Shield complaint cannot be resolved through the above channels, under certain conditions, you may invoke binding arbitration for some residual claims not resolved by other redress mechanisms. See Privacy Shield Annex 1 at https://www.privacyshield.gov/article?id=ANNEX-I-introduction.

Personal information means any information relating to an identified or identifiable natural person in line with the definition of "Personal Information" under the EU General Data Protection Regulation and "personal information" under the California Consumer Privacy Act.

This Policy applies to all personal information which is collected and processed as part of the regular business activities of Company in the course of providing services to a data controller, owner, other third party, or another Group Member (equally referred to as the "**Customer**" in this Policy). When applicable, regular business activities may include processing by Company of personal information contained within customer support tickets processed via Company's platform.

Group Members and their employees (including new hires and individual contractors) must comply with this Policy when collecting and processing personal information in their capacity as service providers.

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

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

PART I: BACKGROUND AND ACTIONS

WHAT IS DATA PROTECTION LAW?

Data protection law gives individuals 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 the national data protection authorities, federal or state authorities, and the courts. When Company collects and uses personal information to provide a service, this activity, and the personal information in question is covered and regulated by data protection law.

When an organization collects, uses or transfers personal information for its own purposes, or determines the purposes and means of the processing of Personal Information, that organization is deemed to be a "*controller"* of that information and is therefore primarily responsible for meeting the legal requirements under data protection law.

On the other hand, when an organization processes personal information on behalf of a third party (for example, personal information processed on behalf of a Company enterprise customer) or a different member of its corporate group (for example, to provide an intercompany service) that organization is deemed to be a "*processor"* of the information. In this case, the relevant controller of the personal information (i.e. the relevant third party or group member) will be primarily responsible for meeting the legal requirements.

This Policy describes how Company will comply with data protection law in respect of processing it performs as a processor. Company's Global Personal Information Handling Procedures: Controller Policy describes the standards Company applies when Company collects, uses or transfers personal information as a controller.

HOW DOES DATA PROTECTION LAW AFFECT COMPANY NATIONALLY AND INTERNATIONALLY?

European data protection law does not allow the transfer of personal information to countries outside Europe that do not ensure an adequate level of data protection. For the purpose of this Policy reference to Europe means the EEA and U.K. Some of the countries in which Company operates are not regarded by European data protection authorities as providing an adequate level of protection for individuals' privacy and data protection rights. From a national perspective, individual state law, such as the California Consumer Privacy Act, will obligate Company to treat personal information in compliance with law.

When Company acts as a processor, Company's Customers in Europe retain the responsibility to comply with European data protection law. Certain data protection obligations are passed on to Company in the contracts Company has with its Customers. Consequently, if Company fails to comply with the terms of the contracts it enters into with its Customers, Company's Customers may be in breach of applicable data protection law and Company may face a claim for breach of contract, which may result in the payment of compensation or other judicial remedies.

In such cases, if an individual demonstrates that it has suffered damage, and that it is likely that the damage has occurred due to a breach of this Policy by Company outside Europe (or a third

party sub-processor established outside Europe), the Company entity accepting liability (namely rMark Bio, Inc.) will be responsible for demonstrating that the Group Member outside Europe (or the third party sub-processor established outside Europe) is not responsible for the breach, or that no such breach took place.

WHAT IS COMPANY DOING ABOUT IT?

Company must take proper steps to ensure that it uses personal information on an international basis in a safe and lawful manner. This Policy therefore sets out a framework to satisfy data protection law requirements and in particular, to provide an adequate level of protection for all personal information used and collected in Europe and transferred to Group Members outside Europe, either where the personal information is collected by a Customer in Europe as a controller, or where the personal information is collected by Company in Europe as a processor.

Each of Company's Customers must decide whether the commitments made by Company in this Policy provide adequate safeguards for the personal information transferred to Company under the terms of its contract with Company. Company will apply the rules contained in this Policy whenever it acts as a processor for a Customer. Where Company's Customers rely upon this Policy as providing adequate safeguards, upon request, a copy of this Policy will be incorporated into the contract with those Customers. If a Customer chooses not to rely upon this Policy that Customer is responsible for putting in place another adequate safeguard to protect the personal information.

Company will apply this Policy in all cases where Company processes personal information as a processor both manually and by automatic means.

This Policy applies to all Group Members and their employees worldwide (including new hires and individual contractors), and they must comply with, and respect, this Policy when collecting and using personal information as a processor. All Group Members who collect, use or transfer personal information to provide services to a third party, or who provide a service to other Group Members, in their capacity as a processor, must comply with the Rules set out in **Part II** of this Policy together with the policies and procedures set out in the appendices in **Part III** of this Policy.

Some Group Members may act as both a controller and a processor and must therefore comply with this Policy and also the as appropriate.

FURTHER INFORMATION

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

Attention: Chief Privacy Officer

Email:privacy@rmarkbio.com

Address: 222 W. Merchandise Mart
Plaza Suite 1230
Chicago IL 60654

Attn: Chief Privacy Officer

The Company Information Governance Council is responsible for ensuring that changes to this Policy are notified to the Group Members and to individuals whose personal information is processed by Company in accordance with Appendix 8.

If you are unhappy about the way in which Company has used your personal information, Company has a separate complaint handling procedure which is set out in Part III, Appendix 6.

PART II: PROCESSOR OBLIGATIONS

This Policy applies in all situations where Company collects, uses and transfers personal information as a processor.

Part II of this Policy is divided into three sections:

- Section A addresses the basic principles that Company must observe when it collects, uses and transfers personal information as a processor.

- Section B deals with the practical commitments made by Company in connection with this Policy.

- Section C describes the third party beneficiary rights that Company has granted to individuals in its capacity as a processor under this Policy.

SECTION A: BASIC PRINCIPLES

RULE 1 – COMPLIANCE WITH LOCAL LAW

Rule 1A – Company will ensure that compliance with this 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 than is provided for in this Policy, Company acknowledges that it will take precedence over this Policy.

Rule 1B – Company will cooperate and assist a controller to comply with its obligations under applicable data protection laws in a reasonable time and to the extent reasonably possible.

Company will, within a reasonable time and as required under the terms of the contracts with its Customers, assist Customers to comply with their obligations as controllers under applicable data protection laws. This may include, for example, a responsibility to comply with certain instructions stipulated in the contract with a Customer, such as providing assistance to that Customer to meet its obligations to keep personal information accurate and up to date.

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

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

Company's Customers have a duty to explain to individuals, at the time their personal information is collected, or shortly after, how that information will be used. This is usually done by means of an easily accessible fair processing statement. Company will provide such assistance and information to its Customers as may be required under the terms of its contracts with its Customers to comply with this requirement. For example, Company may be required

to provide information about any sub-processors appointed by Company to process Customer personal information on its behalf under the terms of a contract with a particular Customer.

Rule 2B – Company will only use personal information on behalf of, and in accordance with, the instructions of the controller.

Company will only use personal information on behalf of its Customers and in compliance with the terms of the contracts with its Customers.

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

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

In the event that legislation prevents Company from returning the personal information to a Customer, or destroying it, Company will maintain the confidentiality of the personal information and will not process the personal information otherwise than in accordance with the terms of its contract with that Customer.

RULE 3 – DATA QUALITY AND PROPORTIONALITY

Rule 3 – Company will assist controllers to keep the personal information accurate and up to date.

Company will comply with any instructions from a Customer, as required under the terms of its contract with that Customer, in order to assist that Customer to comply with its obligation to keep personal information accurate and up to date.

When required to do so on instruction from a Customer, as required under the terms of its contract with that Customer, Company will delete, anonymize, update or correct personal information.

Company will notify other Group Members or any third party sub-processor to whom the personal information has been disclosed accordingly so that they can also update their records.

In practice, when Company acts for a Customer in its capacity as the provider of a helpdesk ticketing platform, Company does not have access to the personal information of Customers' data subjects and so when acting in this capacity Company is unlikely to be required to delete, anonymize, update or correct such personal information.

RULE 4 – RESPECTING INDIVIDUALS' RIGHTS

Rule 4 – Company will assist controllers to comply with the rights of individuals.

Company will act in accordance with the instructions of a Customer as required under the terms of its contract with that Customer and undertake any reasonably necessary measures to enable a Customer to comply with its duty to respect the rights of individuals. In particular, if any Group Member receives a subject access request, the Group Member will transfer such request promptly to the relevant Customer and not respond to such a request unless authorized to do so or required by law. Company will follow the steps set out in the Subject Access Request Procedure (see Appendix 2) when dealing with such requests.

RULE 5 – SECURITY AND CONFIDENTIALITY

Rule 5A – Company will put in place appropriate technical and organizational measures to safeguard personal information processed on behalf of a controller.

European data protection law expressly requires that where Company provides a service to a Customer which involves the processing of personal information, the contract between Company and its Customer controls the security and organizational measures required to safeguard that information consistent with the law of the European country applicable to the Customer.

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

Group Members will notify a Customer of any security breach in relation to personal information processed on behalf of that Customer without undue delay and as required to do so under the terms of the Group Member's contract with that Customer.

Rule 5C – Company will comply with the requirements of a controller regarding the appointment of any sub-processor.

Company will inform its Customers where processing undertaken on their behalf will be conducted by a sub-processor and will comply with the particular requirements of a Customer with regard to the appointment of sub-processors as set out under the terms of its contract with that Customer. Company will ensure that up to date information regarding its appointment of sub-processors is available to those Customers at all times so that their general consent is obtained. If, on reviewing this information, a Customer objects to the appointment of a sub-processor to process personal information on its behalf, that Customer will be entitled to take such steps as are consistent with the terms of its contract with Company and as referred to in Rule 2B of this Policy.

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

Group Members must only appoint sub-processors who provide sufficient guarantees in respect

of the commitments made by Company in this Policy. In particular, such sub-processors must be able to provide appropriate technical and organizational measures that will govern their use of the personal information to which they will have access in accordance with the terms of the Group Member's contract with its Customer.

To comply with this Rule, where a sub-processor has access to personal information processed on behalf of Company, Company will take steps to ensure that it has in place appropriate technical and organizational security measures to safeguard the personal information and will impose strict contractual obligations, in writing, on the sub-processor, which provide:

- commitments on the part of the sub-processor regarding the security of that information, consistent with those contained in this Policy (and in particular Rules 5A and 5B above) and with the terms of the contract Company has with its Customer in respect of the processing in question;

- that the sub-processor will act only on Company's instructions when using that information; and

- such obligations as may be necessary to ensure that the commitments on the part of the sub-processor reflect those made by Company in this 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 Company in Europe to a sub-processor established outside Europe.

SECTION B: PRACTICAL COMMITMENTS RULE 6 – COMPLIANCE

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

Company has appointed its Chief Privacy Officer to oversee and ensure compliance with this Policy. The Chief Privacy Officer is supported by the Company Privacy Counsel, which is responsible for overseeing and enabling day-to-day compliance with this Policy at a regional and compliance level. A summary of the roles and responsibilities of Company's privacy team is set out in Appendix 3.

RULE 7 – TRAINING

Rule 7 – Company 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 4.

RULE 8 – AUDIT

Rule 8 – Company will comply with the Audit Protocol set out in Appendix 5.

RULE 9 – COMPLAINTS

Rule 9 – Company will comply with the Complaint Handling Procedure set out in Appendix 6.

RULE 10 – CO-OPERATION

Rule 10 – Company will comply with the Co-operation Procedure set out in Appendix 7.

RULE 11 – UPDATES TO THE POLICY

Rule 11 – Company will comply with the Updating Procedure set out in Appendix 8.

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

Rule 12A – Company will ensure that where it believes that the legislation applicable to it prevents it from fulfilling its obligations under this Policy, Company will promptly inform (unless otherwise prohibited by law):

- **the controller as provided for by Rule 2B (unless otherwise prohibited by a law enforcement authority)**
- **the Chief Privacy Officer**
- **the appropriate data protection authority competent for the controller**

Rule 12B – Company will ensure that where it receives a legally Personal Information Handling request for disclosure of personal information which is subject to this Policy, Company will:

- **notify the controller promptly unless prohibited from doing so by a law enforcement authority; and**
- **put the request on hold and notify the lead data protection authority and the appropriate data protection authority competent for the controller, unless legally prohibited from doing so or where there is an imminent risk of serious harm.**

If Company receives a legally Personal Information Handling request for disclosure of personal information which is subject to this Policy, Company will:

- notify the controller promptly unless prohibited from doing so by a law enforcement authority; and

- put the request on hold and notify the lead data protection authority and the appropriate data protection authority competent for the controller, unless legally prohibited from doing so or where there is an imminent risk of serious harm.

If Company is legally prohibited from putting the request on hold, it will inform the requesting authority about its obligations under European data protection law and ask the authority to waive this prohibition. Where such prohibition cannot be waived, Company will provide the competent data protection authorities with an annual report providing general information about any such requests for disclosure it may have received, to the extent legally permitted to do so.

SECTION C: THIRD PARTY BENEFICIARY RIGHTS

Under European data protection law, individuals whose personal information is processed in Europe by Company acting as a processor (an "**EEA Entity**") and/or transferred to Company located outside Europe under the Policy (a "**Non-EEA Entity**") have certain rights. These individuals may enforce the Policy as third party beneficiaries where they cannot bring a claim against a controller in respect of a breach of any of the commitments in this Policy by Company (or by a sub-processor) acting as a processor because:

(i) the controller has factually disappeared or ceased to exist in law or has become insolvent; and

(ii) no successor entity has assumed the entire legal obligations of the controller by contract or by operation of law.

In such cases, the individual's rights are as follows:

(a) *Complaints*: Individuals may complain to an EEA Entity in accordance with the Complaint Handling Procedure and/or to a European data protection authority in the jurisdiction of the transferring EEA Entity;

(b) *Liability:* Individuals may bring proceedings against Company International Ltd: (i)in the courts of Ireland; (ii) in the jurisdiction from which the personal information was transferred; or (iii) in the courts of the jurisdiction of the EEA Member State where the individual resides;

(c) *Compensation:* Individuals may seek appropriate redress from Company International Ltd (including the remedy of any breach of the Processor Policy by a Non-EEA Entity) and where appropriate, receive compensation from Company International Ltd for any damage suffered as a result of a breach of this Policy by: (i) a Non-EEA Entity; (ii)any third party processor which is established outside the EEA and which is acting on behalf of an EEA Entity or a Non-EEA Entity, or (iii) in accordance with the determination of the court or other competent authority;

(d) *Transparency:* Individuals may obtain a copy of this Policy and the Intra-group Agreement entered into by Company in connection with this Policy from Company International Ltd or any other EEA Entity on request.

Where a Non-EEA Entity acts as a processor on behalf of a Customer, then if an individual or the Customer suffers damage and can demonstrate that it is likely that the damage has occurred because of a breach of this Policy, the burden of proof to show that (i) a Non-EEA Entity; or (ii) any third party sub- processor who is established outside the EEA who is acting on behalf of a Non-EEA Entity is not responsible for the breach, or that no such breach took place, will rest with Company International Ltd.

Company International Ltd will ensure that any action necessary is taken to remedy any breach of the Processor Policy by a Non-EEA Entity or any third party processor which is established outside the EEA and which is processing personal information on behalf of a controller.

PART III: APPENDICES

APPENDIX 1

PRIVACY SHIELD PRINCIPLES

rMark Bio, Inc. complies with the EU-U.S. Privacy Shield Framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information transferred from the European Union and United Kingdom (UK) to the United States. rMark Bio, Inc. has certified to the U.S. Department of Commerce that it adheres to the Privacy Shield Principles. If there is any conflict between the terms in this privacy policy and the Privacy Shield Principles, the Privacy Shield Principles shall govern. To learn more about the Privacy Shield program, and to view our certification, please visit https://www.privacyshield.gov/.

rMark Bio is a Chicago, Illinois-based healthcare innovation services provider. rMark Bio believes healthcare is best served when individuals with diverse backgrounds come together with a common purpose and clear objectives to improve patient lives. We are product strategists, engineers, data scientists and designers who are experts in our domain and passionate about advancing life sciences for the greater good. Bio advisors provide diverse expertise in finance, business strategies, and the pharmaceutical industry. rMark Bio collects the following types of personally identifiable information: name, physical address, company issued identification numbers, country of residence, fax number, phone number, email address, professional designation, and in some cases geolocations data. rMark Bio does not sell personally identifiable information, and will only share personally identifiable information with our third-party service providers under strict agreement to protect such information. This personally identifiable information is used to provide service related information to client's and the individual our clients contract with. Personal information is not sold or disclosed to unauthorized third-party, however, rMark Bio may disclose personally identifiable information in connection with lawful requests by public authorities, including to meet national security or law enforcement requirements. With respect to personal data received or transferred pursuant to the Privacy Shield Frameworks, Company is subject to the regulatory investigative, and enforcement powers of the U.S. Federal Trade Commission.

In compliance with the Privacy Shield Principles, rMark Bio, Inc. commits to resolve complaints about our collection or use of your personal information. EU and UK individuals with inquiries or complaints regarding our Privacy Shield policy should first contact rMark Bio at: privacy@rmarkbio.com.

rMark Bio, Inc has further committed to refer unresolved privacy complaints under the Privacy Shield Principles to an independent dispute resolution mechanism, the BBB EU PRIVACY SHIELD. If you do not receive timely acknowledgment of your complaint, or if your complaint is not satisfactorily addressed, please visit http://www.bbb.org/EU-privacy-shield/for-eu-consumers for more information and to file a complaint. This service is provided free of charge to you.

If your Privacy Shield complaint cannot be resolved through the above channels, under certain conditions, you may invoke binding arbitration for some residual claims not resolved by other

redress mechanisms. See Privacy Shield Annex 1 at https://www.privacyshield.gov/article?id=ANNEX-I-introduction.

1. NOTICE

a. Company will provide Notice as set forth in the processor procedures that will inform individuals about:

i. its participation in the Privacy Shield and provide a link to, or the web address for, the Privacy Shield List,

ii. the types of personal data collected and, where applicable, the entities or subsidiaries of the organization also adhering to the Principles,

iii. its commitment to subject to the Principles all personal data received from the EU in reliance on the Privacy Shield,

iv. the purposes for which it collects and uses personal information about them,

v. how to contact the organization with any inquiries or complaints, including any relevant establishment in the EU that can respond to such inquiries or complaints,

vi. the type or identity of third parties to which it discloses personal information, and the purposes for which it does so,

vii. the right of individuals to access their personal data,

viii. the choices and means the organization offers individuals for limiting the use and disclosure of their personal data,

ix. the independent dispute resolution body designated to address complaints and provide appropriate recourse free of charge to the individual, and whether it is: (1) an alternative dispute resolution provider based in the EU, or (2) an alternative dispute resolution provider based in the United States,

x. being subject to the investigatory and enforcement powers of the FTC, or any other U.S. authorized statutory body,

xi. the possibility, under certain conditions, for the individual to invoke binding arbitration,

xii. the requirement to disclose personal information in response to lawful requests by public authorities, including to meet national security or law enforcement requirements, and

xiii. its liability in cases of onward transfers to third parties.

b. This notice will be prominently featured in clear and conspicuous language when

individuals are first asked to provide personal information to the organization or as soon thereafter as is practicable, but in any event before Company uses such information for a purpose other than that for which it was originally collected or processed by the transferring organization or discloses it for the first time to a third party.

2. CHOICE

a. Company will offer individuals the opportunity to choose (opt-out) whether their personal information is: (i) to be disclosed to a third party; or (ii) to be used for a purpose that is materially different from the purpose(s) for which it was originally collected or subsequently authorized by the individuals. Where applicable, individuals will be provided with clear, conspicuous, and readily available mechanisms to exercise choice.

b. By derogation to the previous paragraph, it is not necessary to provide choice when disclosure is made to a third party that is acting as an agent to perform task(s) on behalf of and under the instructions of the organization. However, Company shall always enter into a contract with the agent.

c. For sensitive information (i.e., personal information specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or information specifying the sex life of the individual), Company will obtain affirmative express consent (opt-in) from individuals if such information is to be (i) disclosed to a third party or (ii) used for a purpose other than those for which it was originally collected or subsequently authorized by the individuals through the exercise of opt-in choice. In addition, an organization should treat as sensitive any personal information received from a third party where the third party identifies and treats it as sensitive.

3. ACCOUNTABILITY FOR ONWARD TRANSFER

To transfer personal information to a third party acting as a controller, organizations must comply with the Notice and Choice Principles. Company must also enter into a contract with the third-party controller that provides that such data may only be processed for limited and specified purposes consistent with the consent provided by the individual and that the recipient will provide the same level of protection as the Principles and will notify the organization if it makes a determination that it can no longer meet this obligation. The contract shall provide that when such a determination is made the third-party controller ceases processing or takes other reasonable and appropriate steps to remediate.

To transfer personal data to a third-party acting as an agent, Company will: (i) transfer such data only for limited and specified purposes; (ii) ascertain that the agent is obligated to provide at least the same level of privacy protection as is required by the Principles; (iii) take reasonable and appropriate steps to ensure that the agent effectively processes the personal information transferred in a manner consistent with the organization's obligations under the Principles; (iv) require the agent to notify the organization if it makes a determination that it can no longer meet its obligation to provide the same level of protection as is required by the Principles; (v) upon notice, including under (iv), take reasonable and appropriate steps to stop and remediate unauthorized processing; and (vi) provide a summary or a representative copy of the relevant privacy provisions of its contract with that agent to the Department upon request.

In certain situations, we may be required to disclose personal data in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.

4. SECURITY

As an organization that is creating, maintaining, using or disseminating personal information, Company will take reasonable and appropriate measures to protect it from loss, misuse and unauthorized access, disclosure, alteration and destruction, taking into due account the risks involved in the processing and the nature of the personal data.

5. DATA INTEGRITY AND PURPOSE LIMITATION

a. Consistent with the Principles, personal information must be limited to the information that is relevant for the purposes of processing. Company will not process personal information in a way that is incompatible with the purposes for which it has been collected or subsequently authorized by the individual. To the extent necessary for those purposes, Company will take reasonable steps to ensure that personal data is reliable for its intended use, accurate, complete, and current. Company will adhere to the Principles for as long as it retains such information.

b. Information may be retained in a form identifying or making identifiable the individual only for as long as it serves a purpose of processing within the meaning set forth above. This obligation does not prevent Company from processing personal information for longer periods for the time and to the extent such processing reasonably serves the purposes of archiving in the public interest, journalism, literature and art, scientific or historical research, and statistical analysis. In these cases, such processing shall be subject to the other Principles and provisions of the Framework. Company will take reasonable and appropriate measures in complying with this provision.

6. ACCESS

Company will have in place rules and policies that will endures that individuals will have access to personal information about them that Company holds and will be able to correct, amend, or delete that information where it is inaccurate, or has been processed in violation of the Principles, except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question, or where the rights of persons other than the individual would be violated. In order to exercise your rights please write to us at privacy@rmarkbio.com.

7. RECOURSE, ENFORCEMENT AND LIABILITY

a. Company's privacy protection will include robust mechanisms for assuring compliance with the Principles, recourse for individuals who are affected by non-compliance with the Principles, and consequences for Company when the Principles are not followed. At a minimum such mechanisms must include:

i. readily available independent recourse mechanisms by which each individual's complaints and disputes are investigated and expeditiously resolved at no cost to the

individual and by reference to the Principles, and damages awarded where the applicable law or private-sector initiatives so provide;

ii. follow-up procedures for verifying that the attestations and assertions organizations make about their privacy practices are true and that privacy practices have been implemented as presented and, in particular, with regard to cases of non-compliance; and

iii. obligations to remedy problems arising out of failure to comply with the Principles by organizations announcing their adherence to them and consequences for such organizations. Sanctions must be sufficiently rigorous to ensure compliance by organizations.

b. Company and its selected independent recourse mechanisms will respond promptly to inquiries and requests by the Department for information relating to the Privacy Shield. Company will respond expeditiously to complaints regarding compliance with the Principles referred by EU Member State authorities through the Department.

c. Organizations are obligated to arbitrate claims and follow the terms invoking binding arbitration by delivering notice to the organization at issue and following the procedures and subject to conditions set forth the dispute resolution mechanism.

d. In the context of an onward transfer, a Company acknowledges that it has responsibility for the processing of personal information it receives under the Privacy Shield and subsequently transfers to a third party acting as an agent on its behalf. Company shall remain liable under the Principles if its agent processes such personal information in a manner inconsistent with the Principles, unless Company proves that it is not responsible for the event giving rise to the damage.

e. The Company is subject to the investigatory and enforcement powers of the Federal Trade Commission (FTC). If Company becomes subject to an FTC or court order based on non-compliance, the Company shall make public any relevant Privacy Shield-related sections of any compliance or assessment report submitted to the FTC, to the extent consistent with confidentiality requirements. The FTC will give priority consideration to referrals of non-compliance with the Principles from the Department and EU Member State authorities, and will exchange information regarding referrals with the referring state authorities on a timely basis, subject to existing confidentiality restrictions. In certain circumstance there is a possibility, under certain conditions, a data subject with a dispute may be able to invoke binding arbitration.

APPENDIX 2

SUBJECT ACCESS REQUEST PROCEDURE

Personal Information Handling Procedures:

Subject Access Request Procedure

Personal Information Handling Procedures: Subject Access Request Procedure

2. Introduction

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

2.2. When Company acts as a controller, individuals whose personal information is collected and/or used in Europe (even if subsequently transferred to other Group Members) are entitled to have communicated to them whether any personal information about them is being processed by Company, and if so, to obtain a copy of that personal information. This is known as the right of subject access. In this Procedure, Europe means the EEA **and** Switzerland

2.3. In addition, all individuals whose personal information is collected and / or used in Europe by Company acting as controller, and transferred between Company group members ("**Group Members**") under the Personal Information Handling Procedures: Controller Policy, will also benefit from the right of subject access. Such subject access requests will be dealt with in accordance with the terms of this Personal Information Handling Procedures: Subject Access Request Procedure ("**Procedure**").

2.4. This Procedure explains how Company deals with a subject access request relating to personal information which falls into the categories in sections 1.2 and 1.3 above (referred to as "**valid request**" in this Procedure).

2.5. Where a subject access request is subject to European data protection law because it is made in respect of personal information collected and/or used in Europe, such a request will be dealt with by Company in accordance with this Procedure, but where the applicable European data protection law differs from this Procedure, the local data protection law will prevail.

3. Individuals' rights

3.1. An individual making a valid subject access request to Company when Company is a controller of the personal information requested is entitled:

(a) to be informed whether Company holds and is processing personal information about that person;

(b) to be given a description of the categories of personal information processed, the purposes for which they are being held and processed and the recipients or classes of recipients to whom the information is, or may be, disclosed by Company; and

(c) to communication in intelligible form of the personal information held by Company.

3.2. The request must be made in writing, which can include email. Unless the local data protection law provides that an oral request may be made, in which case Company will document the request and provide a copy to the individual making the request before dealing with it. Company must respond to a valid request within forty (40) calendar days (or any shorter period as may be stipulated under local law) of receipt of that request.

3.3. Company is not obliged to comply with a subject access request unless Company is supplied with such information which it may reasonably require in order to confirm the identity of the individual making the request. To assist it in fulfilling the subject access request in an efficient and timely manner, it may also communicate with the individual with a view to gathering information that will help it to locate the information which that person seeks.

4. Process

Receipt of a subject access request when Company is a controller of the personal information requested.

4.1. If Company receives any request from an individual for their personal information, this must be passed to the Company Information Governance Council at dsr@rmarkbio.com immediately upon receipt indicating the date on which it was received together with any other information which may assist the Company Information Governance Council to deal with the request.

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

Initial steps

4.3. The Company Information Governance Council will make an initial assessment of the request to decide whether it is a valid request and whether confirmation of identity, or any further information, is required. It will also engage Company Personnel for support with handling the subject access, as required or appropriate.

4.4. The Company Information Governance Council will then contact the individual in writing to confirm receipt of the subject access request, seek confirmation of identity or further information, if required, or decline the request if one of the exemptions to subject access applies.

5. Exemptions to the right of subject access for requests made to Company as a controller

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

(a) Where the subject access request is made to a European Group Member, if the refusal to provide the information is consistent with the data protection law within the jurisdiction in which that Group Member is located; or

(b) Where the subject access request is made to a non-European Group Member and the refusal to provide the information is consistent with the exemptions to the right of subject access under current EU data protection laws.

(c) Where the personal information is held by Company in non-automated form that is not or will not become part of a filing system.

(d) Where the personal information does not originate from Europe, has not been processed by any European Group Member, and the provision of the personal information requires Company to use disproportionate effort.

5.2. The Company Information Governance Council will assess each request individually to determine whether any of the above-mentioned exemptions applies.

6. Company's search and the response

6.1. The Company Information Governance Council will arrange a search of all relevant electronic and paper filing systems.

6.2. The Company Information Governance Council may refer any complex cases to the Chief Privacy Officer for advice, particularly where the request includes information relating to third parties or where the release of personal information may prejudice commercial confidentiality or legal proceedings.

6.3. The information requested will be collated by the Company Information Governance Council into a readily understandable format (internal codes or identification numbers used at Company that correspond to personal information shall be translated before being disclosed). A covering letter will be prepared by the Company Information Governance Council which includes information required to be provided in response to a subject access request.

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

7. Subject access requests made to Company where Company is a processor of the personal information requested

7.1. When Company processes information on behalf of a Customer (for example, to provide a service), Company is considered to be a *processor* of the information and the

Customer will be primarily responsible for meeting the legal requirements as a controller. This means that when Company acts as a processor, Company's Customers retain the responsibility to comply with applicable data protection law.

7.2. Certain data protection obligations are passed to Company in the contracts Company has with its Customers and Company must act in accordance with the instructions of its Customers and undertake any reasonably necessary measures to enable its Customers to comply with their duty to respect the rights of individuals. This means that if any Group Member receives a subject access request in its capacity as a processor for a Customer that Group Member must transfer such request promptly to the relevant Customer and not respond to the request unless authorized by the Customer to do so.

7.3. Company may have additional responsibilities to individuals in the EU and the UK based on its self-certification under the Privacy Shield Framework in instances where the access request concerns information received in the United States in reliance on Privacy Shield.

8. Requests for erasure, amendment or cessation of processing of personal information

8.1. If a request is received for the erasure, amendment, or cessation of processing of an individual's personal information where Company is the controller for that personal information, such a request must be considered and dealt with as appropriate by the Company Information Governance Council.

8.2. If a request is received advising of a change in an individual's personal information where Company is the controller for that personal information, such information must be rectified or updated accordingly if Company is satisfied that there is a legitimate basis for doing so.

8.3. When Company deletes, anonymizes, updates, or corrects personal information, either in its capacity as controller or on instruction of a Customer when it is acting as a processor, Company will notify other Group Members or any sub-processor to whom the personal information has been disclosed accordingly so that they can also update their records.

8.4. If the request made to Company as a controller is to cease processing that individual's personal information because the rights and freedoms of the individual are prejudiced by virtue of such processing by Company, or on the basis of other compelling legitimate grounds, the matter will be referred to the Company Information Governance Council to assess. Where the processing undertaken by Company is required by law, the request will not be regarded as valid.

8.5. All queries relating to this Procedure are to be addressed to the Company Information Governance Council or at dsr@rmarkbio.com

APPENDIX 3

COMPLIANCE STRUCTURE

Personal Information Handling Procedures: Privacy Compliance Structure

1. Introduction

1.1. Company's compliance with data protection laws and the "Personal Information Handling Procedures: Controller Policy" and "Personal Information Handling Procedures: Processor Policy" (together the "**Policies**" or, respectively, the "**Controller Policy**" and the "**Processor Policy**") is overseen and managed throughout all levels of the business by a multi-layered, cross-functional privacy compliance structure. Further information about Company's Information Governance Council is set out below and a list of the current members of the Company Information Governance Council is provided at Appendix 1.

2. Role of the Information Governance Council

2.1. *Information Governance Council role:* The Company group of companies ("**Company**") have established a privacy compliance team (the "**Information Governance Council**") whose role is to ensure and oversee Company's compliance with data protection and information security requirements. It will achieve this through the fulfillment of its responsibilities described below.

2.2. *Board reporting:* The Information Governance Council will report and make recommendations to Company senior management and the Board of Directors (the "**Board**") on a regular basis concerning:

- Company's compliance with legal and regulatory requirements concerning data protection and information security;

- the content, implementation and effectiveness of Company's data protection and information security policies and processes; and

- any data protection and information security incidents experienced, the measures taken to remedy or mitigate those incidents, and the steps taken to prevent their reoccurrence.

3. Information Governance Council Composition

3.1. *Membership of the Information Governance Council:* The Information Governance Council shall consist of a cross-functional group of senior staff members from various Company offices (see Appendix 1 for current members).

3.2. *New members:* Additional or replacement members of the Information Governance Council shall be nominated and approved by majority approval of the Information Governance Council. The Chief Privacy Officer shall have the casting vote in the event of a tied vote.

4. Meetings

4.1. *Frequency of meetings:* The Information Governance Council shall meet at least once per quarter, and more often if the Information Governance Council deems it necessary to carry out its responsibilities under this Charter, to address a change in applicable legal or regulatory requirements or to respond to a data protection or information security incident.

4.2. *Quorum and voting requirements:* A majority of the members of the Information Governance Council shall constitute a quorum for purposes of holding a meeting and the Information Governance Council may act by a vote of a majority of the members present at such meeting. The Chief Privacy Officer shall have the casting vote in the event of a tied vote.

5. Responsibilities of the Information Governance Council

5.1. *Responsibilities:* The Information Governance Council will have the following responsibilities and authority:

A. Accountability

- The Information Governance Council shall be accountable for managing and implementing Company's compliant data protection and information security practices and procedures within Company, and for ensuring that effective data protection and information security controls exist whenever Company discloses personal information to a third party service provider.

- The Information Governance Council will serve as a central contact point for any data protection related questions or concerns (via the contact e-mail address privacy@rmarbio.com), whether raised by internal Company staff members or external Company customers and suppliers, and will oversee the resolution of those questions or concerns.

B. Review of data protection policies and procedures

- The Information Governance Council will evaluate, implement and oversee data protection and information security compliance practices within Company that are consistent with the requirements of applicable laws and Company's policies, strategies and business objectives.

- The Information Governance Council will periodically assess Company's data protection and information security compliance measures, accomplishments, and resources to ensure their continued effectiveness and identify and action improvements where necessary.

- The Information Governance Council may discuss with senior management the data protection and information security legal and regulatory requirements applicable to Company and its compliance with such requirements. After these discussions, the Information Governance Council may, where it determines it appropriate, make recommendations to the Chief Privacy Counsel (who, in turn, will report any material amendments or modifications to the Board) with respect to Company's data protection and information security policies and procedures to ensure ongoing compliance with applicable laws and regulations.

- The Information Governance Council will also periodically review and assess the continued effectiveness and adequacy of this Charter. Where necessary, it will recommend to the Chief Privacy Officer any amendments or modifications it believes are necessary (who, in turn, will report any material amendments or modifications to the Board).

C. Training and awareness raising

- The Information Governance Council will be responsible for instituting and overseeing the adequacy of Company's data protection training program for Company staff that have access to personal information.

- The Information Governance Council will promote privacy awareness across all business units, functional areas and geographies through data protection communications and awareness-raising initiatives.

- The Information Governance Council shall ensure that any updates to its data protection and information security policies are communicated to staff and, where required, Company customers and data protection authorities.

D. Audits

- The Information Governance Council will provide input on audits undertaken of Company's data protection and information security policies and procedures, coordinating responses to audit findings and responding to audit enquiries of its internal or external auditors, data protection authorities, and Company customers.

E. Annual performance evaluation

- The Information Governance Council shall once a year evaluate its own performance and report the findings and recommendations of such evaluation to the Chief Privacy Officer.

F. Risk assessment

- The Information Governance Council shall regularly assess whether Company's data protection and information security policies, procedures and guidance expose Company to any material compliance risks and, where this is the case, identify the steps that Company may take to mitigate or remedy such risks.

- The Information Governance Council may discuss with senior management legal matters (including pending or threatened litigation) that may have a material effect on Company's finances, reputation or its data protection and information security compliance policies and procedures.

G. Engagement of Advisors

- The Information Governance Council may engage independent counsel and such other advisors it deems necessary or advisable to help it perform its responsibilities for data protection and information security.

Appendix 3: Members of the Company Information Governance Council

Name	Title	Department
Brian Ganaway	Chief Privacy Officer and EVP	Operations
David A. Wheeler	Legal Counsel	Legal
Harriet Tran	Director of Product	Product
David Van Able	Data Steward	Team Human
Jason Smith	Head of Engineering	Engineering
Jason Nett	VP of Data Science	Data Science
Joe Bangah	VP of Finance and Human Resources	Human Resources

CONFIDENTIAL

APPENDIX 4

PRIVACY TRAINING REQUIREMENTS

Personal Information Handling Procedures: Privacy Training Requirements

6. Background

6.1. The "Personal Information Handling Procedures: Controller Policy" and "Personal Information Handling Procedures: Processor Policy" (together the "Policies" or, respectively, the "Controller Policy" and the "Processor Policy") provide a framework for the transfer of personal information between Company group members ("**Group Members**"). The purpose of the Privacy Training Requirements document is to provide a summary as to how Company trains its employees and contractors on the requirements of the Policies.

6.2. Company trains employees (including new hires and contractors, whose roles will bring them into contact with personal information) on the basic principles of data protection, confidentiality and information security awareness.

6.3. 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 the Policies and specific data protection issues relevant to their role. This training is further described below and is repeated on a regular basis.

7. Responsibility for the Privacy Training Program

7.1. Company's Information Governance Council has overall responsibility for privacy training at Company, with input with colleagues from other functional areas including Information Security, Human Resources and other departments, as appropriate. They will review training from time to time to ensure it addresses all relevant aspects of the Policies and that it is appropriate for individuals who have permanent or regular access to personal information, who are involved in the collection of personal information or in the development of tools to process personal information.

7.2. Company Management supports the attendance of the privacy training courses, and are responsible for ensuring that individuals within the company are given appropriate time to attend and participate in such courses. Course attendance is monitored via regular audits of the training process. These audits are performed Company's internal audit team and/or independent third-party auditors.

7.3. In the event that these audits reveal persistent non-attendance, this will be escalated to the Chief Privacy Officer for action. Such action may include escalation of non-attendance to the appropriate management authority within Company who will be responsible and held accountable for ensuring that the individual(s) concerned attend and actively participates in such training.

8. About the training courses

8.1. Company has developed mandatory electronic training courses, supplemented by face to face training for employees. The courses are designed to be both informative and use-friendly, generating interest in the topics covered. Employees must correctly answer a series of multiple choice questions for the course to be deemed complete

8.2. All Company employees will be required to complete the training:

(a) as part of their induction program;

(b) as part of a regular refresher training at least once every two years (the timing of which is determined by the Company Information Governance Council); and

(c) when necessary based on changes in the law or to address any compliance issues arising from time to time.

8.3. Certain employees will receive specialist training, including those who are involved in particular processing activities such as employees who work in HR, Marketing, Product Development, Finance/Procurement and Customer Success or whose business activities include processing sensitive Personal Information. Specialist training is delivered as additional modules to the basic training package, which will be tailored depending on the course participants.

9. Training on the Policy

9.1. Company's training on the Policies will cover the following main areas:

9.1.1. Background and rationale:

(a) What is data protection law?

(b) How data protection law will affect Company nationally and internationally

(c) The scope of the Policies

(d) Terminology and concepts.

9.1.2. The Policies:

(a) An explanation of the Policies

(b) Practical examples

(c) The rights that the Policies give to individuals

(d) The privacy implications arising from processing personal information for clients

9.1.3. Where relevant to an employee's role, training will cover the following procedures under the Policies:

(a) Subject Access Procedure

(b) Audit Protocol

(c) Updating Procedure

(d) Cooperation Procedure

(e) Complaint Handling Procedure

10. Further information

10.1. Any queries about training under the Policies should be addressed to Company's Information Governance Council at privacy@rmarkbio.com

CONFIDENTIAL

APPENDIX 5

AUDIT PROTOCOL

Personal Information Handling Procedures: Audit Protocol

11. Background

11.1. Company's "Personal Information Handling Procedures: Controller Policy" and "Personal Information Handling Procedures: Processor Policy" (together the "**Policies**" or, respectively, the "**Controller Policy**" and the "**Processor Policy**") safeguard personal information transferred between the Company group members ("**Group Members**").

11.2. Company must audit its compliance with the Policies on a regular basis, and the purpose of this document is to describe how and when Company will perform such audits.

11.3. The role of Company's Information Governance Council is to provide guidance about the collection and use of personal information subject to the Policies and to assess the collection and use of personal information by Group Members for potential privacy-related risks. The collection and use of personal information with the potential for a significant privacy impact is, therefore, subject to detailed review and evaluation on an on-going basis. Accordingly, although this Audit Protocol describes the formal assessment process adopted by Company to ensure compliance with the Policies as required by the data protection authorities, this is only one way in which Company ensures that the provisions of the Policies are observed and corrective actions taken as required.

12. Approach

Overview of audit

12.1. Compliance with the Policies is overseen on a day-to-day basis by the Company Information Governance Council. The Company Audit Team composed of experienced representatives of Company's Legal, Information Security and Compliance teams ("**Audit Team**") is responsible for performing and/or overseeing independent audits of compliance with the Policies and will ensure that such audits address all aspects of the Policies. The Audit Team is responsible for ensuring that any issues or instances of non-compliance are brought to the attention of the Company Information Governance Council and Chief Privacy Officer and that any corrective actions are determined and implemented within a reasonable time.

12.2. Where Company acts as a processor, Customers (or auditors acting on their behalf) may audit Company for compliance with the commitments made in the Processor Policy and may extend such audits to any sub-processors acting on Company's behalf in respect of such processing, in accordance with the terms of the relevant Customer's contract with Company.

Frequency of audit

12.3. Audits of compliance with the Policies are conducted:

(a) at least annually in accordance with Company's audit procedures;

(b) at the request of the Chief Privacy Officer;

(c) as determined necessary by the Company Information Governance Council (for example, in response to a specific incident); or

(d) (with respect to audits of the Processor Policy), as required by the terms of the relevant Customer's contract with Company.

Scope of audit

12.4. The Audit Team will conduct a risk-based analysis to determine the scope of an audit, which will consider relevant criteria, such as: 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 the personal information processed.

12.5. In the event that a Customer exercises its right to audit Company for compliance with the Processor Policy, the scope of the audit shall be limited to the data processing facilities, data files and documentation relating to that Customer. Company will not provide a Customer with access to systems which process personal information of other Customers.

Auditors

12.6. Audit of the Policies (including any related procedures and controls) will be undertaken by the Audit Team. In addition, Company may appoint independent and experienced professional auditors acting under a duty of confidence as necessary to perform audits of the Policies (including any related procedures and controls) relating to data privacy.

12.7. In the event that a Customer exercises its right to audit Company for compliance with the Processor Policy, such audit may be undertaken by that Customer, or by independent and suitably experienced auditors selected by that Customer, as required by the terms of the relevant Customer's contract with Company.

12.8. In addition Company agrees that European data protection authorities may audit Group Members for the purpose of reviewing compliance with the Policies (including any related procedures and controls) in accordance with the terms of the Personal Information Handling Procedures: Cooperation Procedure.

Reporting

12.9. Data privacy audit reports are submitted to the Chief Privacy Officer and, if the report reveals breaches or the potential for breaches of a serious nature (for example, presenting a risk

of potential harm to individuals or to the business), to the parent Board of Directors.

12.10. Upon request and subject to applicable law and respect for the confidentiality and trade secrets of the information provided, Company will:

(a) provide copies of the results of data privacy audits of the Policies (including any related procedures and controls) to a competent European data protection authority; and

(b) to the extent that an audit relates to personal information Company processes on behalf of a Customer, report the results of any audit of compliance with the Processor Policy to that Customer.

12.11. The Company Information Governance Council is responsible for liaising with the European data protection authorities for the purpose of providing the information outlined in section 2.10.

APPENDIX 6

COMPLAINT HANDLING PROCEDURE

Personal Information Handling Procedures: Complaint Handing Procedure

1. Background

1.1. Company's "Personal Information Handling Procedures: Controller Policy" and "Personal Information Handling Procedures: Processor Policy" (together the "**Policies**" or, respectively, the "**Controller Policy**" and the "**Processor Policy**") safeguard personal information transferred between the Company group members ("**Group Members**"). The purpose of this Complaint Handling Procedure is to explain how complaints brought by an individual whose personal information is processed by Company under the Policies are dealt with.

1.2. This procedure will be made available to individuals whose personal information is processed by Company under the Controller Policy and, where Company processes personal information on behalf of Customers, to those Customers (under the Processor Policy).

2. How individuals can bring complaints

2.1. Individuals can bring complaints in writing by contacting the Company Information Governance Council at privacy@rmarkbio.com

3. Complaints where Company is a controller

Who handles complaints?

3.1. The Company Information Governance Council will handle all complaints arising under the Controller Policy. The Company Information Governance Council will liaise with colleagues from relevant business and support units as appropriate to deal the complaint.

What is the response time?

3.2. Unless exceptional circumstances apply, the Company Information Governance Council will acknowledge receipt of a complaint to the individual concerned within five (5) business days, investigating and making a substantive response within one month.

3.3. If, due to the complexity of the complaint, a substantive response cannot be given within this period, the Company Information Governance Council will advise the complainant accordingly and provide a reasonable estimate (not exceeding six (6) months) for the timescale within which a response will be provided.

What happens if a complainant disputes a finding?

3.4. If the complainant disputes the response from the Company Information Governance Council or any aspect of a finding and notifies the Company Information Governance Council, the matter will be referred to the Chief Privacy Officer. The Chief Privacy Officer 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. The Chief Privacy Officer will respond to the complainant within six (6) months of the receipt of the complaint. As part of the review, the Chief Privacy Officer may arrange to meet the parties to the complaint in an attempt to resolve it.

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

3.6. Individuals also have the right to complain to a competent data protection authority and/or to lodge a claim with a court of competent jurisdiction in accordance with the data protection laws applicable to them, whether or not they have first complained directly to Company.

3.7. The jurisdiction from which the personal information was transferred will determine to which data protection authority a complaint may be made.

3.8. If the matter relates to personal information which was collected and / or used by Company in Europe but then transferred to Company outside Europe and an individual wants to make a claim against Company, the claim may be made against the Group Member in Europe responsible for exporting the personal information.

4. Complaints where Company is a processor

4.1. Where a complaint is brought in respect of the collection and use of personal information where Company is the processor in respect of that information, Company will communicate the details of the complaint to the Customer promptly and will act strictly in accordance with the terms of the contract between the Customer and Company if the Customer requires that Company investigate the complaint. Certain individuals may also have the right to make a complaint under Privacy Shield, as described in Appendix A.

What happens when a Customer ceases to exist?

4.2. In circumstances where a Company Customer has disappeared, no longer exists or has become insolvent, individuals whose personal information is collected and/or used in accordance with European data protection law and transferred between Group Members on behalf of that Customer have the right to complain to Company and Company will handle such complaints in accordance with section 4 of this Complaint Handling Procedure.

4.3. In such cases, individuals also have the right to complain to a European data protection authority and/or to lodge a claim with a court of competent jurisdiction and this includes where they are not satisfied with the way in which their complaint has been resolved by Company. Individuals entitled to such rights will be notified accordingly as part of the complaint handling procedure.

APPENDIX 7

COOPERATION PROCEDURE

Personal Information Handling Procedures: Cooperation Procedure

1. Introduction

1.1. This Personal Information Handling Procedures: Cooperation Procedure sets out the way in which Company will cooperate with the European data protection authorities in relation to the "Personal Information Handling Procedures: Controller Policy" and "Personal Information Handling Procedures: Processor Policy" (together the "**Policies**" or, respectively, the "**Controller Policy**" and the "**Processor Policy**").

2. Cooperation Procedure

2.1. Where required, Company will make the necessary personnel available for dialogue with a European data protection authority in relation to the Policies.

2.2. Company will actively review, consider and (as appropriate) implement:

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

(b) the views of the Article 29 Working Party in connection with Personal Information Handling Procedures for Processors and Personal Information Handling Procedures for Controllers, as outlined in its published Personal Information Handling Procedures guidance.

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

2.4. Company agrees that:

(a) a competent European data protection authority may audit any Group Member located within its jurisdiction for compliance with the Policies, in accordance with the applicable data protection law(s) of that jurisdiction; and

(b) a competent European data protection authority may audit any Group Member who processes personal information for a Customer established within the jurisdiction of that European data protection authority for compliance with the Policies, in accordance with the applicable data protection law(s) of that jurisdiction, with full respect to the confidentiality of the information obtained and to the trade secrets of Company (unless this requirement is in conflict with local applicable law).

2.5. Company agrees to abide by a formal decision of any competent data protection authority against which a right to appeal is not exercised on any issues relating to the interpretation and application of the Policies.

CONFIDENTIAL

APPENDIX 8

UPDATING PROCEDURE

Personal Information Handling Procedures: Updating Procedure

13. Introduction

13.1. This Personal Information Handling Procedures: Updating Procedure sets out the way in which Company will communicate changes to the "Personal Information Handling Procedures: Controller Policy" ("**Controller Policy**") and to the "Personal Information Handling Procedures: Processor Policy" ("**Processor Policy**") (together the "**Policies**") to the European data protection authorities, individual data subjects, its Customers and to the Company group members ("**Group Members**") bound by the Policies.

13.2. Any reference to Company in this procedure is to the Information Governance Council which will ensure that the commitments made by Company in this Updating Procedure are met.

14. Material changes to the Policies

14.1. Company will communicate any material changes to the Policies as soon as is reasonably practical to the Data Protection Commissioner in Ireland and to any other relevant European data protection authorities.

14.2. Where a change to the Processor Policy materially affects the conditions under which Company processes personal information on behalf of any Customer under the terms of its contract with Company, Company will also communicate such information to any affected Customer. If such change is contrary to any term of the contract between Company and that Customer:

(a) Company will communicate the proposed change before it is implemented, and with sufficient notice to enable affected Customers to object; and

(b) Company's Customer may then suspend the transfer of personal information to Company and/or terminate the contract, in accordance with the terms of its contract with Company.

2. Administrative changes to the Policies

2.1. Company will communicate changes to the Policies which:

(a) are administrative in nature (including changes in the list of Group Members); or

(b) have occurred as a result of either a change of applicable data protection law in any European country or due to any legislative, court or supervisory authority measure;

to the Data Protection Commissioner in the relevant European data protection authorities at least once a year. Company will also provide a brief explanation to the Data Protection

Commissioner in Ireland and to any other relevant data protection authorities of the reasons for any notified changes to the Policies.

2.2. In addition, Company will make available changes to the Processor Policy which:

(a) are administrative in nature (including changes in the list of Group Members); or

(b) have occurred as a result of a change of applicable data protection law or due to any legislative, court or supervisory authority measure;

3. Communicating changes to the Policies

3.1. Company will communicate all changes to the Policies, whether administrative or material in nature:

(a) to the Group Members bound by the Policies via written notice (which may include e- mail)*;* and

(b) systematically to Customers and individuals who benefit from the Policies the www.rmarkbio.com website.

3.2. Company will maintain an up to date list of Group Members bound by the Policies and of the sub- processors appointed by Company to process personal information on behalf of Customers. This information will be available on request from Company.

4. Logging changes to the Policies

4.1. The Policies contain a change log which sets out the date each Policy is revised and the details of any revisions made. Company will maintain an up-to-date list of the changes made to the Policies.

5. New Group Members

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