RegenMed

IMPLEMENTATION OF COMMISSION DECISION (EU) 2021/914

November 2023

TABLE OF CONTENTS

1. BACKGROUND

1.1. The Company (the "Company") licenses its patented inCytes™ platform from time to time to companies, healthcare professionals, laboratories, and others (together, inCytes™ Licensees") which may be subject to the General Data Protection Regulation of the European Union (the "GDPR"), including the Commission Decision (EU) 2021/914.

1.2. More information on inCytes™ can be found at https://www.rgnmed.com/company/incytes-tm-technology. More information on the GDPR can be found at https://gdpr-info.eu/. More information on (EU) 2021/914 can be found at https://op.europa.eu/en/publication-detail/-/publication/55862dbf-c72b-11eb-a925-01aa75ed71a1.

1.3. Data collected through inCytes™ by inCytes™ Licensees may include Personal Data and Sensitive Data as defined in the GDPR.

1.4. Data Subjects may be patients being treated, or evaluated for treatment, by inCytes™ Licensees. inCytes™ Licensees and Data Subjects may be located in any EU or non-EU country.

2. PURPOSE

2.1. This Policy describes the manner in which the Company implements the EU 2021/914. Policies governing implementation by the Company of other elements of the GDPR can be found in the Documents Incorporated By Reference section, paragraph below.

3. DEFINITIONS

3.1. All terms not defined in this Document shall have the definitions specified in the GDPR, (EU) 2021/914 and the Documents Incorporated By Reference, paragraph 4 below.

3.2. The Competent Supervising Authority shall be that body identified by the healthcare provider or other inCytes™ Licensee and communicated to the Data Subject.

4. DOCUMENTS INCORPORATED BY REFERENCE

4.1. The following documents to the extent applicable are incorporated herein by reference:

4.1.1. inCytes™ License Agreement (https://kb.rgnmed.com/incytes-license-agreement).

4.1.2. inCytes™ Privacy Policy (https://kb.rgnmed.com/incytes-privacy-policy).

4.1.3. Service™ Provider Agreement (https://kb.rgnmed.com/service-provider-agreement).

4.1.4. inCytes™ Patient Consent (https://kb.rgnmed.com/incytes-patient-consent).

4.1.5. inCytes™ Data Breach Policy (https://kb.rgnmed.com/incytes-data-breach-policy).

4.1.6. GDPR compliance policies of AWS, the subprocessor utilized by the Company, and described more fully at https://aws.amazon.com/compliance/gdpr-center/.

5. LIMITATIONS ON THE COMPANY'S CONTROL

5.1. The Company has no control over, and expressly disavows and control over:

5.1.1. The nature, amount, frequency of capture and other elements of data collected and maintained through inCytes™ by any inCytes™ Licensee.

5.1.2. The relationship between any inCytes™ Licensee and any Data Subject.

5.1.3. The extent to which any inCytes™ Licensees has access to or otherwise utilizes Personal Data outside of the inCytes™ platform.

5.2. In some instances, an inCytes™ Licensees may be considered as a Data Exporter and, in other instances, as a Data Importer. In some instances, the Company may considered as a Data Importer and, in other instances, as a Data Exporter.

6. DATA PROTECTION SAFEGUARDS

6.1. The Company shall process Personal Data solely for the purposes specified in the inCytes™ Privacy Policy. (See paragraph 4, above.) It will only process Personal Data for another purpose where it has obtained the Data Subject's prior consent, where necessary for the establishment, exercise, or defense of legal claims in the context of specific administrative, regulatory, or judicial proceedings, where necessary in order to protect the vital interests of the Data Subject or of another natural person.

6.2. The Company shall make any Personal Data Documents to which it has access through inCytes™ to the Data Subject free of charge. To the extent necessary to protect business secrets or other confidential information, including Personal Data, the Company may redact part of the text of such documents prior to sharing a copy, but shall provide a meaningful summary where the Data Subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Company shall provide the Data Subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

6.3. The Company shall ensure that Personal Data maintained on the inCytes™ platform is accurate and, where necessary, kept up to date, *provided that* any such obligation shall depend on the corresponding compliance with this clause by the relevant inCytes™ Licensee.

6.4. When fulfilling the role of Data Exporter, and subject to the foregoing paragraph, the Company shall:

6.4.1. take every reasonable step to ensure that Personal Data that is inaccurate, having regard to the purpose(s) of processing, is erased or rectified without delay, and

6.4.2. ensure that the Personal Data is adequate, relevant, and limited to what is necessary in relation to the purpose(s) of processing as reflected in its instructions to the Data Importer,

6.4.3. it being recognized that such reasonable steps may call for consultation between the Company and the Data Subject's healthcare provider.

6.5. Subject to the foregoing, if the Company becomes aware that Personal Data it has transferred or received is inaccurate, or has become outdated, it shall inform the relevant inCytes™ Licensee and/or Data Subject as appropriate without undue delay.

6.6. When fulfilling the role of Data Importer, the Company shall retain the Personal Data for no longer than necessary for the purpose(s) for which it is processed. It shall put in place appropriate technical or organizational measures to ensure compliance with this obligation, including erasure or anonymization of the data and all back-ups at the end of the retention period.

7. PROCESSING SECURITY

7.1. When fulfilling the role of Data Exporter, the Company shall, in connection with the transmission of Personal Data, implement appropriate technical and organizational measures to ensure the security of such Personal Data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access (a "Personal Data Breach").

7.2. In assessing the appropriate level of security, the Company shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the Data Subject.

7.3. The Company shall in particular consider having recourse to encryption or pseudonymization, including during transmission, where the purpose of processing can be fulfilled in that manner.

7.4. In the event of a Personal Data Breach concerning Personal Data processed by the Company, it shall take appropriate measures to address the breach, including measures to mitigate its possible adverse effects.

7.5. When fulfilling the role of Data Importer, and in case of a Personal Data Breach under its control which is likely to result in a risk to the rights and freedoms of natural persons, the Company shall without undue delay notify both the Data Exporter and the competent supervisory authority. Such notification shall contain (i) a description of the nature of the breach (including, where possible, categories and approximate number of Data Subjects and Personal Data records concerned), (ii) its likely consequences, (iii) the measures taken or proposed to address the breach, and (iv) the details of a contact point from whom more information can be obtained. To the extent it is not possible for the Company to provide all the information at the same time, it may do so in phases without undue further delay.

7.6. In case of a Personal Data Breach under its control and which is likely to result in a high risk to the rights and freedoms of natural persons, the Company shall also notify without undue delay the Data Subjects concerned of such breach and its nature, if necessary or appropriate through the relevant inCytes™ Licensee(s), together with relevant information, unless the Company has implemented measures to significantly reduce the risk to the rights or freedoms of natural persons, or notification would involve disproportionate efforts. In the latter case, the Company shall instead issue a public communication or take a similar measure to inform the public of the Personal Data Breach.

7.7. For Personal Data Breaches covered by the foregoing paragraphs, the Company or inCytes™ Licensee(s) as appropriate shall document all relevant facts relating to the Personal Data breach, including its effects and any remedial action taken, and keep a record thereof.

8. SENSITIVE DATA

8.1. Where the transfer of data to the Company involves Sensitive Data, and when fulfilling its role as Data Exporter, the Company shall apply specific restrictions and/or additional safeguards adapted to the specific nature of the data and the risks involved. This may include restricting the personnel permitted to access the Personal Data, additional security measures (such as pseudonymization) and/or additional restrictions with respect to further disclosure.

9. ONWARD TRANSFERS

9.1. The Company uses AWS as a subprocessor for Personal Data. The AWS servers utilized by the Company for the processing and maintenance of Personal Data are located in the United States or Canada, as specified by the relevant inCytes™ Licensee. Details on compliance by AWS with GDPR, (EU) 2021/914 and other applicable laws and regulations can be found at https://aws.amazon.com/compliance/gdpr-center/.

9.2. Each inCytes™ Licensee, including Data Subjects, by accessing and using the inCytes™ platform, explicitly consents to the processing of their Personal Data, including Sensitive Data, on such platform. Further information can be found on the inCytes™ Privacy Policy and other documents listed in paragraph 4 above.

9.3. The Company shall remain fully responsible to the relevant inCytes™ Licensee for the performance of the subprocessor's obligations under its contract with the Company. The Company shall notify the relevant inCytes™ Licensee of any failure by the subprocessor to fulfil its obligations under that contract.

10. INSTRUCTIONS FROM DATA EXPORTER TO DATA IMPORTER

10.1. The Company shall process Personal Data only on the basis of documented instructions from an inCytes™ Licensee. The Company may refuse to process Personal Data in the event such instructions are conflicting or unclear, or in the event the Company is otherwise unable to follow those instructions. In those circumstances, the Company shall promptly inform the relevant inCytes™ Licensee.

10.2. The Company shall process the Personal Data only for the specific purpose(s) of the transfer as instructed by the relevant inCytes™ Licensee.

10.3. The Company shall cooperate with and assist the relevant inCytes™ Licensee to enable it to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the Competent Supervisory Authority and the affected Data Subjects, considering the nature of processing and the information available to the Company.

11. DATA SUBJECTS

11.1. The Company shall deal with any enquiries and requests they receive from a Data Subject relating to the processing of his/her Personal Data and the exercise of his/her rights under this Document without undue delay and at the latest within one month of the receipt of the inquiry or request. Any information provided to the Data Subject shall be in an intelligible and easily accessible form, using clear and plain language.

11.2. Where requests from a Data Subject are excessive, in particular because of their repetitive character, the Company may either charge a reasonable fee considering the administrative costs of granting the request or refuse to act on the request.

11.3. The Company may refuse a Data Subject's request if such refusal is allowed under the laws of the country of destination and is necessary and proportionate in a democratic society to protect one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679.

11.4. If the Company intends to refuse a Data Subject's request, it shall inform the Data Subject of the reasons for the refusal and the possibility of lodging a complaint with the Competent Supervisory Authority and/or seeking judicial redress.

11.5. In case of a dispute between a Data Subject and the Company as regards compliance with this Document, the Company shall use its best efforts to resolve the issue amicably in a timely fashion. The Company and the Data Subject shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

11.6. The Company accepts that the Data Subject may be represented by a not-for-profit body, organization or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

11.7. The Company agrees that the choice made by the Data Subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

11.8. The Company shall abide by a decision that is binding under the applicable EU or Member State law.

12. COMMUNICATIONS BY DATA SUBJECTS TO THE COMPANY

12.1. In the event of a communication directly to the Company from a Data Subject requesting the deletion, modification, transfer, or other action with respect to his/her Personal Data, and recognizing that such data may include information relating to the health or treatment of such Data Subject, the Company shall proceed as follows:

12.1.1. The Company shall inform the relevant inCytes™ Licensee of the substance of such communication, without disclosing any Personal Data.

12.1.2. The relevant inCytes™ Licensee shall promptly relay the substance of such communication to any treating healthcare provider to confirm the authenticity of the request. The healthcare provider shall be free in his/her professional judgment to speak with the Data Subject regarding any modification of his/her communication to the Company.

12.1.3. In the event the Data Subject, within fifteen business days of the original communication, does not send a communication to the Company modifying his/her original communication, then the Company shall immediately comply with the original instructions of the Data Subject.

12.1.4. Upon receiving such communication from a Data Subject at any time, the Company shall immediately communicate to that Data Subject explaining the foregoing steps.

13. SUPERVISION

13.1. The Company agrees to submit to the jurisdiction of and cooperate with the Competent Supervisory Authority in any procedures aimed at ensuring compliance with this Document. In particular, the Company agrees to respond to enquiries, submit to audits and comply with the measures adopted by the relevant Competent Supervisory Authority, subject to any right of appeal. The Company shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

13.2. The Company warrants that it has no reason to believe that the laws and practices in the United States of Canada applicable to the processing of the Personal Data, including any requirements to disclose Personal Data or measures authorizing access by public authorities, prevents it from fulfilling their obligations under this Document. This is based on the understanding that 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) of Regulation (EU) 2016/679, are not in contradiction with this Document.

13.3. The Company has taken due account in particular of the following elements:

13.3.1. the laws and practices of the United States and Canada – including those requiring the disclosure of data to public authorities or authorizing access by such authorities – relevant in light of the specific circumstances of an onward transfer, and the applicable limitations and safeguards; and

13.3.2. any relevant contractual, technical, or organizational safeguards put in place to supplement the safeguards under this Document, including measures applied during transmission and to the processing of the Personal Data in the country of destination.

13.4. The Company agrees to document the assessment under the foregoing paragraphs and to make such documents available to the Competent Supervisory Authority on request.

13.5. The Company agrees to notify inCytes™ Licensees subject to the GDPR promptly if, after having agreed to this Document and for its duration, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements contained herein, including following a change in the laws of the United States or Canada or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with such requirements.

13.6. Following a notification pursuant to the preceding paragraph, the Company shall promptly identify appropriate measures (e.g. technical or organizational measures to ensure security and confidentiality) to be adopted to address the situation. The Company shall, and an inCytes™ Licensee shall be free, to suspend Onward Transfers if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the Competent Supervisory Authority to do so. In this case, an inCytes™ Licensee shall be entitled to terminate any contract with the Company, insofar as it concerns the processing of Personal Data.

14. NOTIFICATION

14.1. The Company agrees to notify a relevant inCytes™ Licensee and, where possible, the Data Subject promptly (if necessary, with the help of that inCytes™ Licensee) if it:

14.1.1. receives a legally binding request from a public authority, including judicial authorities, under the laws of the United States or Canada for the disclosure of Personal Data; or

14.1.2. becomes aware of any direct access by public authorities to Personal Data in accordance with the laws of the United States or Canada.

14.2. Any notification required by the preceding paragraph shall include information about the Personal Data requested, the requesting authority, the legal basis for the request and the response provided.

14.3. If the Company is prohibited from notifying an inCytes™ Licensee or Data Subject, it agrees to 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. The Company will document its best efforts in order to be able to demonstrate them on request of an inCytes™ Licensee or Data Subject.

14.4. Where permissible under the laws of the United States or Canada, the Company agrees to provide to the relevant inCytes™ Licensee, at regular intervals for the duration of the license, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

14.5. The Company will preserve the information described in the foregoing paragraphs and allowed to be communicated, for the duration of the contract and make it available to the Competent Supervisory Authority on request.

14.6. The foregoing paragraphs are without prejudice to the obligation of any Data Importer to inform a Data Exporter promptly when it is unable to comply with this Document.

15. FINAL PROVISIONS

15.1. At any time, on behalf of itself or any Data Subject, an inCytes™ Licensee may terminate the Onward Transfer to the Company of Personal Data.

15.2. Upon the request of a Data Subject, and subject to the procedures set out in paragraph 12, the Company shall, at the choice of the Data Subject, return his/her Personal Data or delete it and any copies thereof in their entirety.

15.3. The Company shall certify the deletion of the Personal Data to the Data Subject. Until the Personal Data is deleted or returned, the Company shall continue to ensure compliance with this Document. In case of local laws applicable to the Company which prohibit the return or deletion of the transferred Personal Data, the Company warrants that it will continue to ensure compliance with this Document and will only process the data to the extent and for as long as required under that local law.

15.4. Any inCytes™ Licensee or Data Subject may revoke its agreement to be bound by this Document where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of Personal Data to which this Document applies; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the Personal Data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

15.5. Data Subjects may invoke and enforce this Document, as third-party beneficiaries, against the Company or an inCytes™ Licensee, except as provided in (EU) 2016/679, (EU) 2021/94 and other governing EU regulations.

15.6. This Agreement pertains only to rights and obligations of Data Subjects covered by the GDPR. It does not pertain to any other rights and obligations.

15.7. The frequency of data transfer to which this Document pertains is determined by the inCytes™ Licensees.

15.8. The technical and organizational measures undertaken by the Company to ensure the security of Personal Data can be found at https://aws.amazon.com/compliance/gdpr-center/.