Processor Agreement

concerning

Provision of an ELN

between

Blank University of Technology

and

Research Innovations Ltd

PROCESSOR AGREEMENT

Between:

BLANK UNIVERSITY OF TECHNOLOGY, located at [ ],

hereinafter "**Controller**"

And

Research Innovations Ltd, of 16 Charlotte Square, Edinburgh, EH2 4DF, Scotland United Kingdom, herein duly represented by Rory Macneil,

hereinafter "**Processor**"

CONTENTS

Whereas:

A. On <DATE>, the Parties concluded an agreement with reference <REFERENCE OF THE AGREEMENT> concerning provision of an electronic lab notebook for pilot use by researchers at Controller. In performance of the agreement, the Processor processes Personal Data on behalf of the Controller;
B. Within the context of the performance of the Agreement, Research Innovations Ltd is deemed a Processor within the meaning of the GDPR and Blank University of Technology is deemed a Controller within the meaning of the GDPR;
C. The Parties want to treat the Personal Data that are or will be processed for the performance of the Agreement with due care and in accordance with the GDPR and other Applicable Legislation and Regulations concerning the Processing of Personal Data;
D. In accordance with the GDPR and other Applicable Legislation and Regulations concerning the Processing of Personal Data, the Parties want to lay down their rights and obligations in respect of the Processing of the Data Subjects' Personal Data In Writing in this Processor Agreement.

have agreed as follows

1 DEFINITIONS

The capitalised terms used in this Processor Agreement have the meaning given in this article. Where the singular is used in the definition in this article, this is understood to include the plural, and vice versa, unless otherwise is explicitly indicated or shown by the context.

1.1 **Agreement**: the agreement concluded between the Controller and the Processor and on the basis of which the Processor processes Personal Data for the Controller for the purpose of the performance of this agreement.
1.2 **Annex**: an annex to this Processor Agreement, which forms an integral part of this Processor Agreement.
1.3 **Applicable Legislation and Regulations concerning the Processing of Personal Data**: the applicable legislation and regulations and/or (further) treaties, regulations, directives, decrees, policy rules, instructions and/or recommendations from a competent public body concerning the Processing of Personal Data, also including future amendments of and/or supplements thereto, including laws of the Member States implementing the GDPR and the Telecommunications Act.
1.4 **Data Subject**: the identified or identifiable natural person to whom the Personal Data pertain, as referred to in Article 4 at 1) GDPR.
1.5 **Employee**: the employees and other persons engaged by the Processor for whose activities it is responsible and who are engaged by the Processor for the performance of the Agreement.
1.6 **GDPR**: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the Processing of Personal Data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
1.7 **In Writing**: laid down in writing or by electronic means, as referred to Article 6:277a of the Dutch Civil Code.
1.8 **Personal Data**:all information relating to a Data Subject; a natural person who can be directly or indirectly identified, in particular based on an identifier such as a name, an

identification number, an online identifier or one or more elements that are characteristic of the physical, physiological, genetic, psychological, economic, cultural or social identity of that natural person, as referred to in Article 4 at 1) GDPR, is deemed identifiable.

1.9 **Personal Data Breach**: (suspicion of) a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed, as referred to in Article 4 at 12) GDPR.

1.10 **PIA**: the data protection impact assessment (privacy impact assessment) performed prior to the Processing in respect of the impact of the intended processing activities on the protection of the Personal Data, as referred to in Article 35 GDPR.

1.11 **Processing**: any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction, as referred to at Article 4 at 2) GDPR.

1.12 **Processor Agreement**: the present agreement including Annexes, as referred to in Article 28(3) GDPR.

1.13 **Recipient**: a natural or legal person, public authority, agency or another body, whether or not a Third Party, to whom/which the Personal Data are disclosed, as referred to in Article 4 at 9) GDPR.

1.14 **Service**: the service(s) to be provided by the Processor to the Controller based on the Agreement.

1.15 **Special categories of Personal Data**: Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, and genetic data, biometric data for the purpose of uniquely identifying a natural person, or data concerning health or data concerning a natural person's sex life or sexual orientation, as referred to in Article 9 GDPR.

1.16 **Sub-processor**: another processor, including but not limited to group companies, sister companies, subsidiaries and auxiliary suppliers, engaged by the Processor to perform specific processing activities at the Controller's expense.

1.17 **Supervisory Authority**: one or more independent public bodies responsible for supervising the application of the GDPR, in order to protect the constitutional rights and fundamental freedoms of natural persons in connection with the Processing of their Personal Data and to facilitate the free traffic of Personal Data inside the Union, as referred to in Article 4 at 21) and Article 51 GDPR. In the Netherlands, this is the Dutch Data Protection Authority (Autoriteit Persoonsgegevens).

1.18 **Third Party**: a natural or legal person, public authority, agency or body other than the Data Subject, the Controller or the Processor, or the person who, under the direct authority of the Controller or Processor, is authorised to process Personal Data, as referred to in Article 4 at 10) GDPR.

2 SUBJECT OF THE PROCESSOR AGREEMENT

2.1 The Processor Agreement forms a supplement to the Agreement and replaces any arrangements agreed earlier between the Parties in respect of the Processing of Personal Data. In the event of any conflict between the provisions of the Processor Agreement and the Agreement, the provisions of the Processor Agreement prevail.

2.2 The general provisions from the Processor Agreement apply for all Processing in the performance of the Agreement. The Processor shall immediately notify the Controller if the

Processor has reason to assume that the Processor can no longer comply with the Processing Agreement.

2.3 The Controller shall give the Processor assignments and instructions for processing the Personal Data on behalf of the Controller. The Controller's instructions are described in more detail in the Processor Agreement and the Agreement. The Controller may issue reasonable supplementary or deviating instructions In Writing.

2.4 The Processor shall process the Personal Data exclusively on assignment from the Controller and on the basis of instructions from the Controller. The Processor shall exclusively process the Personal Data in so far as the processing is necessary for the performance of the agreement, and never for its own use, the use of Third Parties and/or other purposes, unless applicable Union law or provisions of Member State law oblige the Processor to perform Processing. In that event, the Processor shall notify the Controller of this provision In Writing prior to the Processing, unless that legislation prohibits such notification for serious reasons of public interest.

2.5 The Processor and the Controller shall comply with the GDPR and other Applicable Legislation and Regulations concerning the Processing of Personal Data. The Processor shall immediately notify the Controller if, in the opinion of the Processor, an instruction from the Controller breaches the GDPR and/or other Applicable Legislation and Regulations concerning the Processing of Personal Data.

2.6 If the Processor determines the purpose and means of the Processing of Personal Data in violation of the Processor Agreement and/or the GDPR and/or other Applicable Legislation and Regulations concerning the Processing of Personal Data, the Processor is deemed the Controller for that Processing.

3 PROCESSING OF PERSONAL DATA

3.1 Before concluding the Processor Agreement, the Processor shall completely and truthfully inform the Controller in Annex A about the Processing that the Processor conducts in the performance of the agreement, unless Annex A provides that the Controller enters the relevant information in this Schedule. The Processor is exclusively entitled to perform the Processing specified in Annex A.

4 PROVIDING ASSISTANCE AND COOPERATION

4.1 The Processor shall provide the Controller with all necessary assistance and cooperation in complying with the obligations borne by the Parties on the basis of the GDPR and other Applicable Legislation and Regulations concerning the Processing of Personal Data. The Processor shall provide the Controller with assistance in any event in respect of:

(i) Protection of Personal Data;
(ii) Performance of verifications and audits;
(iii) Performance of PIAs;
(iv) Prior consultation with the Supervisory Authority;
(v) Compliance with requests from the Supervisory Authority or another public body;
(vi) Compliance with requests from Data Subjects;
(vii) Reporting Personal Data Breaches.

4.2 Providing assistance and cooperation in respect of compliance with requests from Data Subjects is understood to include, but is not limited to, the following obligations for the Processor:

4.2.1 The Processor shall take all reasonable measures to ensure that the Data Subject can exercise his rights.

4.2.2 If, in relation to the exercise of his rights, a Data Subject contacts the Processor directly, the Processor shall not (substantively) respond - unless expressly instructed otherwise by the Controller - but shall immediately report this to the Controller, with a request for further instructions.

4.2.3 If the Processor offers the Service directly to the Data Subject, the Processor is obliged to inform the Data Subject on behalf of the Controller about the Processing of the Data Subject's Personal Data in a manner that is in accordance with the Data Subject's rights.

4.3 Providing assistance and cooperation in respect of compliance with requests from the Supervisory Authority or another public body is understood to include, but is not limited to, the following obligations for the Processor:

4.3.1 If the Processor receives a request or order concerning Personal Data from a Dutch and/or foreign public body, including but not limited to a request from the Supervisory Authority, the Processor shall immediately notify the Controller in so far as this is permitted by law. When handling the request or order, the Processor shall observe all of the Controller's instructions and provide to the Controller all reasonably required cooperation.

4.3.2 If the Processor is prohibited by law from complying with its obligations on the basis of Clause 4.3.1, the Processor shall promote the Controller's reasonable interests. This is understood to include, but is not limited to:

4.3.2.1 The Provider shall procure a legal assessment of the extent to which (i) the Processor is required by law to comply with the request or order; and (ii) the Processor is in fact prohibited from complying with its obligations to the Controller based on Clause 4.3.1.

4.3.2.2 The Processor shall only cooperate with the request or order if the Processor is required by law to do so, and the Processor shall object where possible (by legal action) to the request or order or the injunction against informing the Controller in this respect or against following the Controller's instructions.

4.3.2.3 The Processor shall not provide any more Personal Data than strictly necessary to comply with the request or order.

4.3.2.4 If there is transfer within the meaning of Clause 9, the Processor shall investigate the possibilities for complying with Articles 44 through 46 GDPR.

5 ACCESS TO PERSONAL DATA

5.1 The Processor shall limit access to Personal Data by Employees, Sub-processors, Third Parties and other Recipients of Personal Data to a necessary minimum.

5.2 The Processor shall exclusively provide access to Employees who must have this access to Personal Data in the performance of the Agreement. The categories of Employees are specified in Annex A.

5.3 The Processor shall not provide Sub-processors access to Personal Data without previous general or specific consent In Writing from the Controller. General consent In Writing for the engagement of Sub-processors is only given if this is expressly included in Annex A. Specific

consent In Writing for the engagement of Sub-processors is only given to Sub-processors who are specified in Annex A.

5.4 The Processor shall notify the Controller in the event of general consent In Writing for the engagement of Sub-processors no later than three (3) months before the intended changes in respect of the addition, replacement or change in Sub-processor(s), In Writing, offering the Controller the possibility of objecting to these changes. The Parties will subsequently enter into negotiations.

5.5 The Controller's general or specific consent for the engagement of Sub-processors does not prejudice the Processor's obligations ensuing from the Processor Agreement, including but not limited to Clause 9. The Controller may withdraw its general or specific consent In Writing for the engagement of Sub-processors if the Processor does not satisfy or no longer satisfies the obligations under the Processor Agreement, the GDPR and/or other Applicable Legislation and Regulations concerning the Processing of Personal Data.

5.6 At the Controller's first request, the Processor shall provide to the Controller a list of the Sub-processors engaged by the Processor.

5.7 The Processor shall impose the obligations included in the Processor Agreement on the (legal) persons engaged by the Processor, including but not limited to Employees and/or Sub-processors. The Processor shall ensure that the (legal) persons engaged by the Processor, including but not limited to Employees and/or Sub-processors, comply with the obligations included in the Processor Agreement by means of an agreement In Writing.

5.8 The Processor shall immediately notify the Controller if the Processor and/or (legal) persons engaged by the Processor, including but not limited to Employees and/or Sub-processors, act in breach of the Processor Agreement and/or of the agreement In Writing concluded with the Processor as referred to in Clause 5.7.

5.9 At the Controller's request, the Processor shall provide the Controller with a copy of the agreement In Writing between the Processor and the (legal) persons engaged by the Processor, including but not limited to Employees and/or Sub-processors.

5.10 In respect of the Controller, the Processor remains completely responsible and completely liable for compliance by the (legal) persons engaged by the Processor, including but not limited to Employees and/or Sub-processors, with the obligations ensuing from the GDPR and/or other Applicable Legislation and Regulations concerning the Processing of Personal Data and the obligations ensuing from the Agreement and the Processor Agreement.

6 SECURITY

6.1 The Processor shall take appropriate technical and organisational measures to safeguard a level of security attuned to the risk, so that the Processing complies with the requirements under the GDPR and other Applicable Legislation and Regulations concerning the Processing of Personal Data, and the protection of the rights of Data Subjects is safeguarded. To this end, the Processor shall take at least the technical and organisational measures included in Annex B.

6.2 In the assessment of the appropriate level of security, the Processor shall take into account the state of the art, the costs of execution, as well as the nature, scope, context and the processing objectives, and the risks varying in terms of probability and seriousness to the rights and freedoms of individuals, especially as a result of the accidental or unlawful destruction, loss, alteration or unauthorised provision of or unauthorised access to data that is transferred, stored or otherwise processed.

6.3 The Processor shall lay down its security policy In Writing. At the Controller's request, the Processor shall allow the Controller to inspect the Processor's security policy.

6.4 Association with an approved code of conduct as referred to in Article 40 GDPR or an approved certification mechanism as referred to in Article 42 GDPR can be used as an element to demonstrate compliance with the requirements referred to in this clause.

7 AUDIT

7.1 The Processor is obliged to periodically have an independent, external expert perform an audit in respect of the Processor's organisation, in order to demonstrate that the Processor complies with the provisions of the Agreement, the Processor Agreement, the GDPR and other Applicable Legislation and Regulations concerning the Processing of Personal Data.

7.2 The Processor shall perform a periodic audit as referred to in Clause 7.1 at least once every two years. If Special Categories of Personal Data are processed, the Processor shall perform a periodic audit as referred to in Clause 7.1 at least once every year.

7.3 The Processor is only not required to perform a periodic audit as referred to in Clause 7.1 if the Processor exclusively processes Personal Data with a low risk and it is expressly laid down in Annex A that the Processor is not required to perform a periodic audit. Whether there is a low risk is determined by the Controller.

7.4 At the Controller's request, the Processor is obliged to make the findings of the independent, external expert available in the form of a statement in which the expert gives an opinion on the quality of the technical and organisational security measures taken by the Processor in respect of the Processing conducted by the Processor on behalf of the Controller.

7.5 At its request, the Controller has the right to have an audit in respect of the Processor's organisation performed by a (legal) person authorised by the Controller, in order to demonstrate that the Processor complies with the provisions of the Agreement, the Processor Agreement, the GDPR and other Applicable Legislation and Regulations concerning the Processing of Personal Data.

7.6 The costs of the periodic audit are at the expense of the Processor. The costs of the audit at the Controller's request are at the Controller's expense, unless the findings of the audit show that the Processor f has failed to comply with the provisions from the Agreement and/or the Processor Agreement and/or the GDPR and/or other Applicable Legislation and Regulations concerning the Processing of Personal Data. This provision does not prejudice the Controller's other rights, including the right to damages.

7.7 If it is established during an audit that the Processor has failed to comply with the provisions of the Agreement and/or the Processor Agreement and/or the GDPR and/or other Applicable Legislation and Regulations, the Processor shall immediately take all measures that are reasonably necessary to ensure the Processor's compliance with these as yet. The accompanying costs are at the Processor's expense.

8 PERSONAL DATA BREACH

8.1 Without unreasonable delay and no later than within 24 hours after discovery, the Processor shall notify the Controller of a Personal Data Breach or a reasonable suspicion of a Personal Data Breach. The Processor shall notify the Controller via the Controller's contact and contact details included in Annex A and at least regarding what is included in Annex C. The Processor warrants that the information provided is complete, correct and accurate.

8.2 If and in so far as it is not possible for the Processor to simultaneously provide all of the information from Annex C, the information may be provided to the Controller step-by-step without unreasonable delay and no later than within 24 hours after the discovery.

8.3 The Processor has organised adequate policy and adequate procedures to detect Personal Data Breaches at the earliest possible stage, to notify the Controller of this no later than within 24 hours, to adequately and immediately respond to this, to prevent or limit (further) unauthorised disclosure, alteration and provision or otherwise unlawful Processing, and to prevent repetition of the same. At the Controller's request, the Processor shall provide information about and allow inspection of this policy organised by the Processor and these procedures organised by the Processor.

8.4 The Processor shall maintain a register In Writing of all Personal Data Breaches that relate to or are connected with the (performance of the) Agreement, including the facts regarding the Personal Data Breach, its consequences and the corrective measures taken. At the Controller's request, the Processor shall provide the Controller with a copy of this register.

9 TRANSFER OF PERSONAL DATA

9.1 Personal Data may be transferred to third countries or international organisations only if there is an appropriate level of protection and the Controller has given specific consent for this In Writing. This specific consent In Writing is only granted if this is included in Annex A. The Processor is exclusively entitled to these transfers to third countries or international organisations specified in Annex A, unless a provision under Union law or under Member State law requires the Processor to perform Processing. In that event, the Processor shall notify the Controller of this provision In Writing prior to the Processing, unless that legislation prohibits such notification for serious reasons of general interest.

9.2 The Controller may attach further conditions to the consent In Writing as referred to in Clause 9.1, including but not limited to demonstrating that the requirements included in Clause 9.3 have been satisfied.

9.3 The Controller may only give the Processor consent for a transfer of Personal Data to third countries or international organisations if either:

(i) An adequacy decision in accordance with Article 45(3) GDPR has been taken in respect of the third country involved or the international organisation involved; or

(ii) Appropriate safeguards in accordance with Article 46 GDPR, including binding rules as referred to in Article 47 GDPR, have been taken in respect of the third country involved or the international organisation involved; or

(iii) One of the specific conditions from Article 49(1) GDPR has been met in respect of the third country involved or the international organisation involved.

10 CONFIDENTIALITY OF PERSONAL DATA

10.1 All Personal Data are qualified as confidential and must be treated as such.

10.2 The Parties shall keep all Personal Data confidential and shall not disclose them in any way, either internally or externally, except in so far as:

(i) Disclosure and/or provision of the Personal Data is necessary in the context of the performance of the Agreement or the Processor Agreement;

(ii) Any mandatory statutory provision or court decision requires the Parties to disclose and/or provide the Personal Data, in which case the Parties shall first notify the other Party of this;

(iii) Disclosure and/or provision of the Personal Data takes place with prior consent In Writing from the other Party.

10.3 Breach of Clause 10.1 and/or Clause 10.2 is deemed a Breach of Personal Data.

11 LIABILITY AND INDEMNIFICATION

11.1 The Processor is liable for all damage ensuing from or in connection with the failure to comply with the Processor Agreement and/or the GDPR and/or other Applicable Legislation and Regulations concerning the Processing of Personal Data.

11.2 The Processor indemnifies the Controller against all claims, penalties and/or measures by third parties, including Data Subjects and the Supervisory Authority, lodged against or imposed on the Controller due to breach of the Processor Agreement and/or the GDPR and/or other Applicable Legislation and Regulations concerning the Processing of Personal Data by the Processor and/or (legal) persons engaged by the Processor, including but not limited to Employees and/or Sub-processors.

11.3 The Processor shall ensure sufficient coverage of the liability by means of liability insurance. At the Controller's request, the Processor shall allow the Controller to inspect the Processor's (policy for this) liability insurance.

12 CHANGES

12.1 The Processor is obliged to immediately notify the Controller of proposed changes in the Service, the performance of the Agreement and the performance of the Processor Agreement that concern the Processing of Personal Data. This is understood to include, but is not limited to:

(i) Changes that (may) affect the Personal Data (categories) to be processed;

(ii) Changes in the means with which the Personal Data are processed;

(iii) The engagement of other Sub-processors;

(iv) Changes in the transfer of Personal Data to third countries and/or international organisations.

12.2 If a change concerning the Processing of Personal Data or an audit gives cause to do so, the Parties shall consult upon the Controller's first request regarding the changes in the Processor Agreement.

12.3 The Processor is only entitled to implement a change in the Service, a change in the performance of the Agreement, a change in the performance of the Processor Agreement and/or a change resulting in amending Annex A if the Controller has given previous consent for such change(s) In Writing.

12.4 Changes that concern the Processing of Personal Data may never result in the Controller being unable to comply with the GDPR and/or other Applicable Legislation and Regulations concerning the Processing of Personal Data.

12.5 In the event of invalidity or avoidability of one or more of the provisions of the Processors Agreement, the other provisions continue to apply in full.

13 TERM AND TERMINATION

13.1 The term of the Processor Agreement is the same as the term of the Agreement. The Processor Agreement cannot be terminated separately from the Agreement. Upon termination of the Agreement, the Processor Agreement terminates by operation of law, and vice versa.

13.2 The Controller is entitled to cancel the Processor Agreement if the Processor does not or can no longer comply with the Processor Agreement, the GDPR and/or other Applicable Legislation and Regulations concerning the Processing of Personal Data, without the Processor being entitled to any damages. When cancelling, the Controller shall observe a reasonable notice period, unless the circumstances justify immediate cancellation.

13.3 Within one month after the Agreement ends, the Processor shall destroy and/or return all Personal Data and/or the Processor shall transfer the same to the Controller and/or another party to be designated by the Controller, at the Controller's discretion. All existing (other) copies of Personal Data, whether or not held by (legal) persons engaged by the Processor, including but not limited to Employees and/or Sub-processors, will also be demonstrably permanently deleted, unless storage of the Personal Data is mandatory under Union or Member State law.

13.4 At the Controller's request, the Processor shall confirm In Writing that the Processor has satisfied all obligations under Clause 13.3.

13.5 The Processor shall bear the costs for the destruction, return and/or transfer of the Personal Data. The Controller may impose additional requirements on the manner of destruction, return and/or transfer of the Personal Data, including requirements on the file format.

13.6 Obligations under the Processor Agreement that are intended by their nature to continue after termination of this Processor Agreement will continue to apply after termination of the Processor Agreement.

14 APPLICABLE LAW AND DISPUTE RESOLUTION

14.1 The Processor Agreement and its performance are governed by the laws of [ ].

14.2 All disputes arising between the Parties in connection with the Processor Agreement shall be submitted to the competent court in the place in which the Controller has its registered office.

Roderick Macneil	<NAME>
Chief Executive	<POSITION>
Research Innovations Ltd	Blank University of Technology

Annex A: Specification of the Processing of Personal Data

In this Annex, the following is set out regarding the Service provided by the Processor:

- Data Subject categories;
- The Personal Data (categories) to be processed;
- Job roles and/or job groups and their Processing;
- Retention periods;
- Security measures taken;
- Auxiliary Suppliers;
- Contact details.

If the Processor offers multiple separate services to the Controller, the information may be included in separate Annexes to be numbered as follows: "Annex A1", "Annex A2", etc.

These Annexes will be attached to the Processor Agreement.

Annex A: Provision of the RSpace electronic lab notebook

Version number [ ], Date of most recent update: [ ].

At time of writing, the entire processing of will be carried out in-house at the TU Blank. This particular contract applies to the transfer of data in relation to usage and support analycs project carried out by RSpace and its sub-processors.

Tranfers
(to be completed by Processor)

Description of the transfer	Entity transferring the Personal Data + country	Entity receiving the Personal Data + country	Transfer mechanism
Support & user analytics	RSpace application	Intercom.io	HTTPS
Analytics	RSpace application	Segment.io	HTTPS

Contact details

For questions on this Annex and/or the Service provided, please contact:

	Controller	Processor
Name		Richard Adams
Position	I	Technical Lead
E-mailadress		richard@researchspace.com
Telephone Number		+447875336302

In the event of a Data Breach, please contact:

	Controller	Processor
Name		Richard Adams
Position	Data Protection Officer	Technical Lead
E-mailadress		richard@researchspace.com
Telephone Number		+447875336302

Annex B: Security measures

Version number 1, Date of most recent update: [ ]

Details of the security measures taken by the Processor *(to be completed by the Processor)*

Security in RSpace

This document explains some of the security procedures and strategies used to keep users' data and details secure.
In general our approach to security is based OWASP recommendations.

Password security

In 'stand-alone' mode (i.e., not using an institutions SSO mechanism to authenticate users), RSpace maintains its own authentication mechanism and credentials database.

- Passwords created by the user must be at least 8 characters long, not be identical to the username, and not belong to a common password blacklist (e.g., 'password'). This blacklist is editable by system administrators.
- Passwords are salted with a unique 16 byte prefix generated by a cryptographically secure random number generator and hashed using the SHA-256 algorithm before persisting to the database. In this way the plaintext password is never stored, and, in the event of the password table becoming compromised, it is not immediately susceptible to dictionary or rainbow table attacks.
- To prevent brute-force password guessing attacks, accounts are locked out for a short time after a number of consecutive unsuccessful logins. All login attempts are logged to a security event log.
- Auto-completion of input fields is disabled for login and signup pages.
- We also recommend that for admin role accounts, end-users follow good practice by disabling password-storing in their browsers.
- After logout, sensitive pages are not cached in the browser.
- Plain-text passwords are never emailed to the user as a result of password reset / forgotten password workflows.

If RSpace is deployed in an institution using SSO, then it is the institution's responsibility to safeguard passwords.

Network security

We recommend that RSpace runs over a secure HTTPS connection which encrypts the communication channel between client and server and also verifies the identity of the endpoint by SSL certificates issued by a recognized Certification Authority. For RSpace instances that we host:

- We use RSA algorithm with 2048 bit key to generate public/private key pairs.
- Require TLS 1.2 protocol (the current recommended versio) for HTTPS transport. No earlier versions are allowed. We plan to support TLS1.3 once low-level libraries that RSpace depends on support the protocol.

- Require AES 128-bit encryption for encrypting the payload.
- Set Strict-Transport-Security Http Header to prevent insecure HTTP connections being attempted
- Require use of ECDHE key exchange protocols that ensure forward secrecy. This ensures that in the event that the server private key is leaked, messages that may have been recorded prior to the leak cannot be decrypted.

We adhere to guidelines issue by the UK National Cyber Security Centreregrding implementation of the TLS protocol. We use one of their recommended tools, Qualys SSL Labs Server Testto scan our sites regularly for TLS vulnerabilities. As of Feb 14th 2018 we rate 'A' standard for our SSL security setup.

Database security

- No direct access to the database is possible by end-users.
- All SQL queries use Prepared Statements to defend against malicious user input.
- The database itself is not encrypted, but OS-level encryption can be used if necessary.
- The RSpace database user runs using limited permissions.

Resource Authorization

Privacy of the user's content depends on RSpace's authorization policy. All access to ELN entries or resources requires authenticated access by default, and URL paths are protected by user roles. At a fine-grained level, access to individual records is controlled by a combination of Access Control Lists (ACLs) and user-specific permissions. Every action (e.g., Read, Edit, Delete, Export, Copy) is authorized at the server level before proceeding - RSpace does not solely rely on controlling the actions available in the UI, as these may be circumvented by URL-guessing attacks.

For example, a user has authorization to edit content created by him/herself, but must be granted permission to access content created by other members of his/her group. To access content created outside a lab group, all PIs or RSpace managers of the groups concerned must accept the sharing request. Otherwise, the content is not accessible. A request to view a record, for example at '/notebook/view/123/' will check for the authenticated user's permission to access record 123 before proceeding.
For more coarse-grained permissions - for example, global admin permissions - we use Role Based Access Control (RBAC) to restrict the available functionality to the user's role.

Defence against malicious use

We are guided by OWASPs guidelines on securing web applications and aim to be at least level 1 compliant in their Application Security Verification Standard (ASVS). Here, we briefly enumerate our policies in the following Control areas:

Authentication & session management (A2)

- Failed logins give no information about reason for failure.
- User names are never used in URLs
- Users are informed at each login when their last login was, so they can see if anyone has impersonated them since their last session.
- A security event logs all login attempts.
- To minimize brute force attacks, accounts are temporarily locked after 3 unsuccessful logins.
- RSpace uses secure random number generators to generate session keys.
- Sessions expire after a short time of inactivity.Users performing sensitive operations must re-authenticate at the time of the operation (e.g., password resets, signing documents, etc)

- Browser caching. Our policy in this are is guided by OWASP's guidelines at (https://www.owasp.org/index.php/Testing_for_Logout_and_Browser_Cache_Management_%28OWASP-AT-007%29). In brief, sensitive data such as login pages, signup pages, user profile pages, and any pages only accessible to a ROLE_ADMIN or ROLE_SYSADMIN are returned from the server with HTTP headers set to prevent browser caching. When a user logs out (or his session expires due to inactivity) the session is invalidated, and clicking on the browser's 'Back' button will trigger a reload from the server for these pages, which will redirect to the login page.

Authorization of resources

- Access to resources is controlled by a combination of Role Base Access Control and instance-based permissions (Access Control Lists)

Cross-Site Request Forgery

- Only same-origin POST requests are permitted

Cross-site scripting

- All user input submitted to the server is filtered before being sent back to the client for display.
- Client side libraries use 'safe' Javascript methods to manipulate user input - e.g., jQuery's text() method.

Injection

- User input is validated
- Exclusive use of prepared statements guards against SQL injection attacks.

Current libraries -A9

- We regularly update libraries and 3rd party software components to ensure the latest security fixes are in place.
- We adopt a SecOps approach, incorporating OWASP's library scanning service into our regular code builds. This cross-references the 3rd party libraries we use against newly reported vulnerabilities.

Security event logging

- *All security events are logged to a dedicated Security log whose output can be consumed by a SEM tool.*

Revision history and audit trail

The *revision history* records all changes made to research records over time. RSpace keeps a full record of this, including timestamps. The *audit trail* records events on the system - document edits and updates are recorded.

Testing and audits
We regularly get CREST-accredited independent penetration testers to evaluate RSpace using manual and automated methods. The latest test was May 2017. We are happy to discuss findings with customers or serious potential customers.

Processor's certificates:
(to be competed by the Processor)

Certifications	Part of organisation / service to which certification pertains	Term of validity of certification	Statement of applicability

Qualifcations satisfied by the Processor: *(to be competed by the Processor)*

Annex C: Information to be provided in the event of a Data Breach

Version number <#>, Date of most recent update: <DATE>

If the Processor must inform the Controller pursuant to Clause 6, it shall provide the following information:

Contact details of reporter

Name	
Position	
E-mailadress	
Telephone Number	

Information on the Data Breach

Provide a summary of the incident, in which the breach of the security of Personal Data occurred
<Fill out>
Of how many persons are Personal Data involved in the breach?
☐ Number: ☐ Minimum: ☐ Maximum:
Describe the group of people whose Personal Data are involved in the breach
<Fill out>
When did the breach take place? (Choose one of the following options and supplement where necessary)
☐ On (date): ☐ Between (startdate and enddate): ☐ Not yet known
What is the nature of the breach? (You can check more than one option)
☐ Reading (confidentiality) ☐ Copying ☐ Changing (integrity) ☐ Removing or destroying (availability) ☐ Theft ☐ Not yet known

What type of Personal Data is involved? (You can check more than one option)
☐ Name and address details ☐ Telephone numbers ☐ E-mail addresses or other addresses for electronic communication ☐ Access- or identifying information (e.g. log-in name/password or client number) ☐ Financial information (e.g. account number, credit card number) ☐ Citizen Service Number (BSN) or taks and social security number ☐ Copies of passport or other identifying documents ☐ Gender, date of birth/or age ☐ Special Personal Data (e.g. race, ethnicity, criminal information, political conviction, trade union membership, religion, seks life, medical details) ☐ Other information, namely (supplement):
What consequences can the breach have for the privacy of the data subjects? (You can check more than one option)
☐ Stigmatisation or exclusion ☐ Damage to health ☐ Exposure to (identity) fraud ☐ Exposure to spam or phishing ☐ Other, namely (provide details):

Follow-up actions in response to the Data Breach

What technical and organisational measure did your organisation take to address the breach and to prevent further breaches?
<Fill out>

Technical protection measures

Have the Personal Data been encrypted, hashed or made incomprehensible or inadmissible to unauthorised persons in any other way? (Choose one of the following options and supplement where necessary)
☐ Yes ☐ No ☐ Partly, namely (supplement):
If all or part of the Personal Data was made incomprehensible or inaccessible, in what manner was this done? (Answer this question if you chose option "Yes" or option "Partly" for the previous question. If you used encryption, also explain the manner of encryption)
<Fill out>

International aspects

Does the breach involve persons in other EU countries? (Choose one of the following options)
☐ Yes ☐ No ☐ Not yet known