[31 OCTOBER 2023]

D5.7 – PROJECT WEBSITE AND LOGO

Version 1.0 – Final
PUBLIC

European Innovation Council

HORIZON-EIC-2022-PATHFINDERCHALLENGES-01 Grant Agreement n°101114899

The project has received funding from the HORIZON-EIC-2022-PATHFINDERCHALLENGES-01 programme under Grant Agreement N° 101114899.

D5.7 PROJECT WEBSITE AND LOGO

Project Acronym:	**Veriqub**
Project Name:	efficient Verification of Quantum computing architectures using Bosons
Grant Agreement No:	**101114899**
Start Date:	**1/09/2023**
End Date:	**31/08/2027**
Contributing WP	**Project management, communication, dissemination and exploitation**
WP Leader:	**INRIA**
Deliverable identifier	**D5.7**
Contractual Delivery Date: 10/2023	**Actual Delivery Date: 10/2023**
Nature: Report	**Version: 1.0 Final**
Dissemination level	**PU**

REVISION HISTORY

VERSION	CREATED/MODIFIER	COMMENTS
0.0	Emilie BLOTIERE (INRIA)	First draft
0.1	Ulysse CHABAUD (INRIA)	Review
1	Emilie BLOTIERE (INRIA)	Final version

TABLE OF CONTENT

TABLE OF ACRONYMS

DPA	Data Processing Agreement
GDPR	General Data Protection Regulation
INRIA	Institut National de Recherche en sciences et technologies du numérique
WP	Work package

TABLE OF FIGURES

PUBLISHABLE SUMMARY

The D5.7 presents the first communication materials of Veriqub project that started first September 2023. It describes the design chart including the project logo, and the creation of the project website. This deliverable is part of the WP5 [Project management, communication, dissemination and exploitation].
The project is funded by HORIZON-EIC-2022-PATHFINDERCHALLENGES-01 programme for 48 months and a maximum grant amount of 3 984 885€. The project is composed of three European beneficiaries (CHALMERS TEKNISKA HOGSKOLA AB, SORBONNE UNIVERSITE, UNIVERSITA DEGLI STUDI DI MILANO) and coordinated by INRIA. The Veriqub project has the ambition to guarantee the reliability and precision of new quantum architectures. Quantum devices offer great promise for computation, cryptography, communication, and sensing. Alternative approaches to quantum information processing in which bosonic modes are the carriers of information have attracted increasing attention, because they offer a hardware-efficient path to fault-tolerance and scalability thanks to their inherently large Hilbert space. However, this poses the problem of providing rigorous guarantees of the correct functioning of these promising bosonic architectures, a task known as quantum verification. To date, this verification is performed by general-purpose tomographic techniques, which rapidly become intractable for large quantum systems. Thus, other methods are needed as quantum devices are scaled up to achieve real-world advantages. Veriqub aims to develop a new approach to the efficient verification of quantum computing architectures with bosons, using continuous-variable measurements.

The name of this research project stands for "efficient Verification of Quantum computing architectures using Bosons". “Bosons” are physical systems that are used as carriers of information, for example, the photons that make up the light of a laser. The main objective of the project is to propose an efficient toolbox for verifying the reliability of quantum computing architectures using bosons. These architectures suffer from reliability issues, even though they could soon outperform conventional computers.

1| VERIQUB GRAPHIC DESIGN

1.1 Visual identity

The Veriqub's visual identity has been created by the French Nicolas Steff company whose director and graphic designer, is used to work with INRIA. His experience of science computing was of paramount importance to draw a simple but expressive identity, easily reusable in any communication support.

FIGURE 1 CHART DESIGN

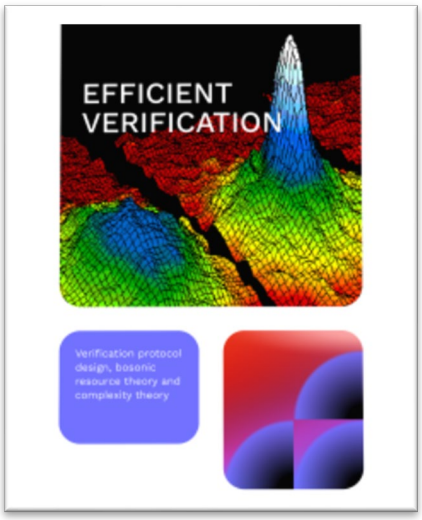

FIGURE 2 CHART ELEMENTS

FIGURE 3 TWITT SIMULATION

The chart design is composed of geometric figures that represent both the cube and the sphere to illustrate the infinitely small that is the atom and the cube to illustrate the project's objective of verifying continuous variables and creating a toolbox.

1.2 Project logo

The logo, shown below in Fig.4 consists on the acronym of the project preceded of a cube with an open window to the project. The cube illustrates both the toolbox, one of the expected outcomes of the project and of course the pun between [cube] and [qubit] (See Fig.6). Qubit is a key concept in quantum information. The quantum bit or qubit is the elementary unit that can carry quantum information. As 1 and 0 are the two states of an ordinary classical bit, a qubit is the coherent superposition of at least two basic quantum states, which can be denoted |0> and |1>. This logo is used in all working documents, internal and external, related to the project and inserted in project templates such as the rolling minutes, deliverables and public presentations. It is stored in different formats (png, jpg and ai) and coloured background (See Fig.5) in the secured project repository NOTION[1] and accessible to the whole consortium. This tool will be described in the D5.8 Plan for dissemination and communication activities due in M6 (end of February 2024).

FIGURE 4 VERIQUB LOGO

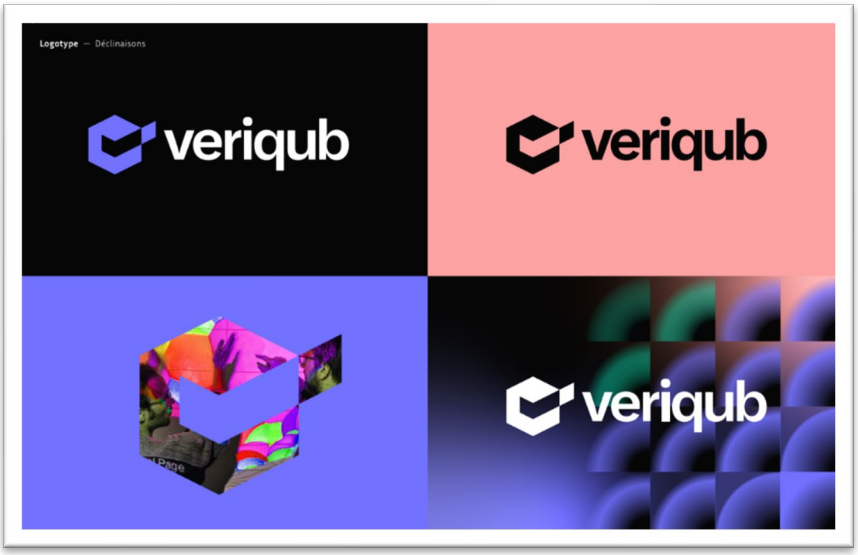

FIGURE 5 COLOURED LOGOS

[1]NOTION: daily project management tool: https://www.notion.so/fr-fr.

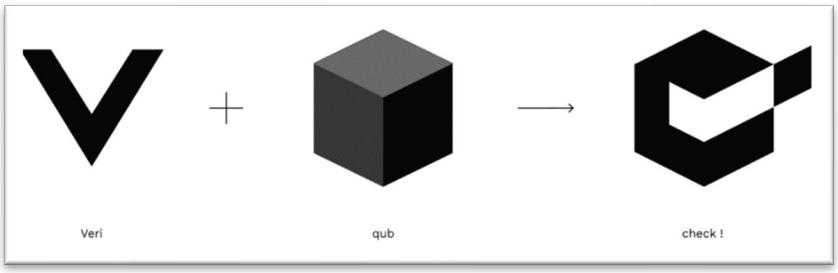

FIGURE 6 LOGO FIGURES

1.3 PowerPoint template

A PowerPoint template is at the disposal of the consortium to use the design chart in their communication activities. The template contains a panel of three different with or without quantum pictures.

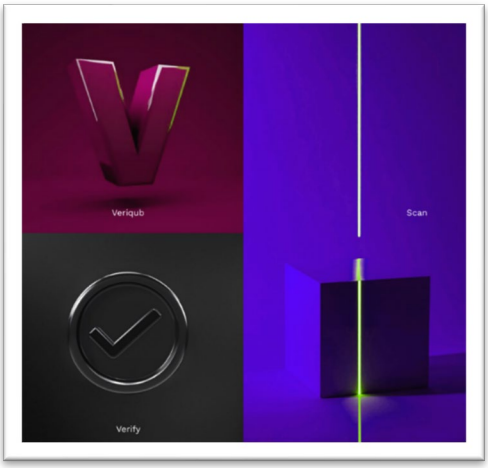

FIGURE 7 INSPIRED FIGURES

FIGURE 8 POWERPOINT TEMPLATE EXAMPLE

1.4 Veriqub Kakemono

FIGURE 9 VERIQUB KAKEMONO

The chart designer also created a chart including a Kakemono to be used for the public presentations. The same colours and figures are used with the synergy of the cube that is the research and the lightened sphere that is the boson, source of energy and light of the atom.

The Kakemono was used for the first time during the kick-off meeting of the project in early October in Paris, in Sorbonne Université premises. The EU legal mentions are at the bottom right of the support and the four partners are mentioned as well.

FIGURE 10 KAKEMONO KEY ELEMENT

2| PROJECT WEBSITE

With a view to optimising and rationalising the use of the project monitoring management tool (Notion, see section 1.1 Project logo), the project website is also being developed using the Notion software, but is harvested on GitHub to remove the Notion header of the website and have clean URLSs. The Data processing addendum of the software is annexed in this deliverable under the Annex 1. The DPA forms part of the Master Subscription Agreement between Notion and its users

2.1 Main pages

So far, the website is made of three main pages, containing subpages:

- Home
- Project
- Partners

The website is updated regularly to reflect key events in the project and keep the community and other interested parties informed. It is a public site, accessible via any search engine, knowing that it takes some time for Google to reference the website.

The website is developed by the scientific coordinator and will be updated only by the coordination team. The software allows for a fast and easy handling and offers flexibility to structure the website in various blocks and depending on the pages.

The *Home* page gives easy access to the recent news, such as the official kick-off meeting and the article launching publicly the project as highlighted in Figures 11 and 12.

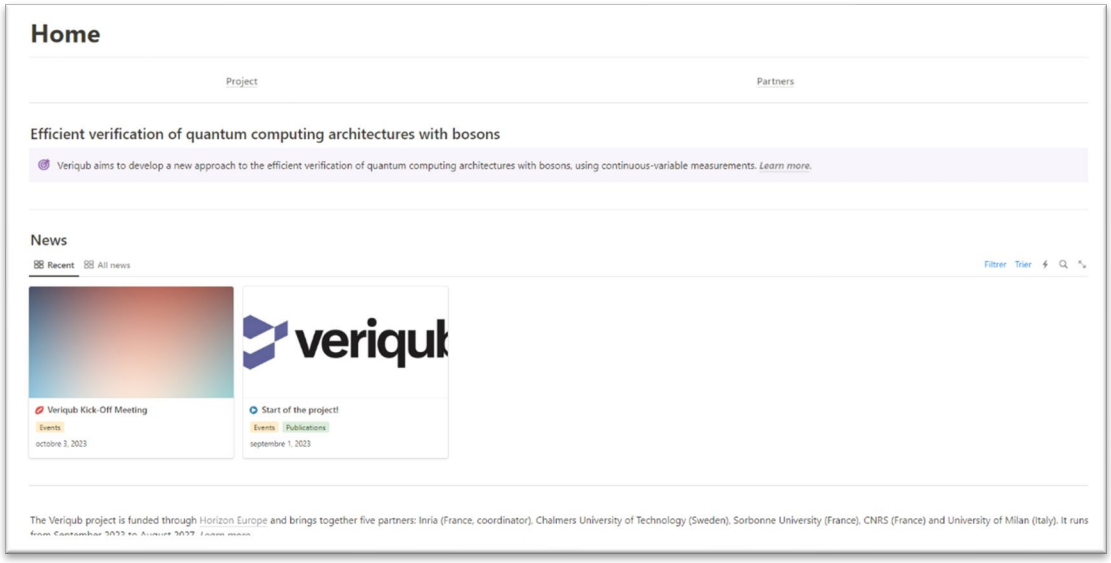

FIGURE 11 PROJECT WEBSITE HOME PAGE

FIGURE 12 KICK OFF SUBPAGE

The *Project* page informs more about the scientific outcomes of the project describing the main objectives (see Fig.13) and giving access to a subpage for the public deliverables. The non-sensible deliverables will be shared in the page after being validated by the European Commission.

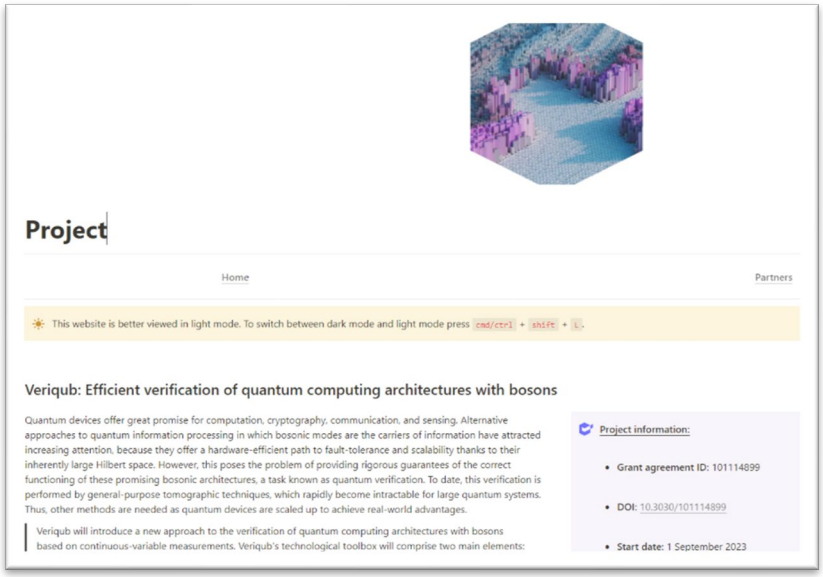

FIGURE 13 PROJECT PAGE

The *Partners* page opens to subpages to learn more about each partner involved in the project as highlighted in Fig.14.

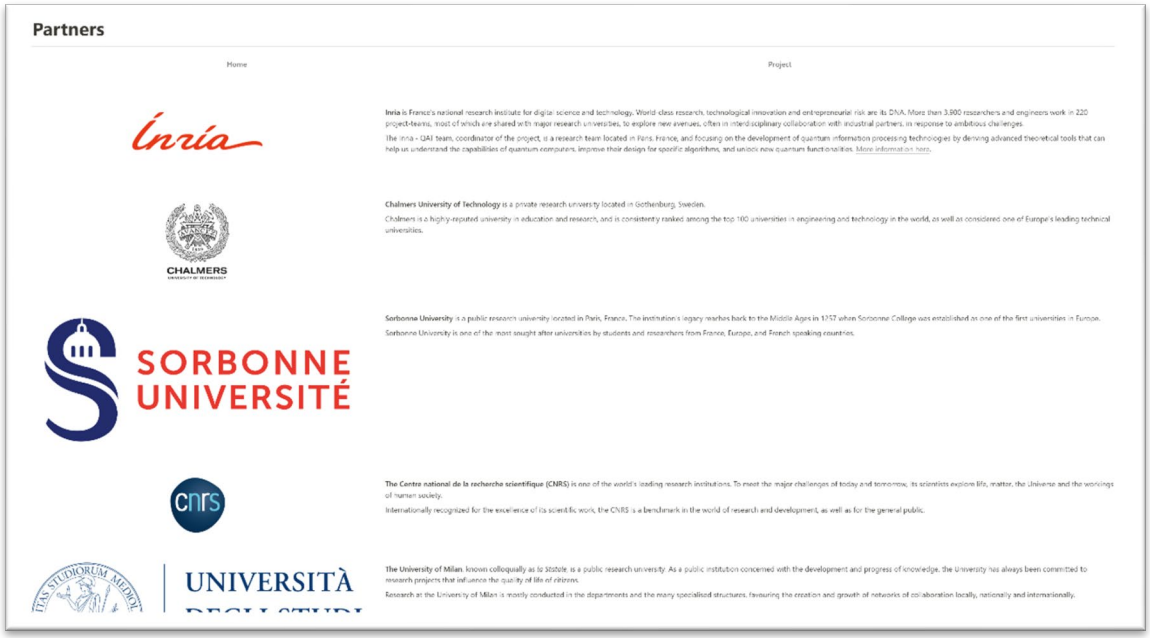

FIGURE 14 PARTNERS PAGE

2.2 Data privacy

2.2.1 RGPD

The website is developed via the Notion device and harvested in Github. Therefore, the website follows the data privacy policy of Notion which is described in the site and accessible to the page: https://www.notion.so/Terms-and-Privacy-28ffdd083dc3473e9c2da6ec011b58ac.GDPR compliance is described in the Data Processing Addendum[2], attached to this deliverable as the Annex. 1.

2.2.2 Privacy policy

The privacy policy of the Notion platform is accessible in the following link: https://www.notion.so/security. The following contact allow to ask about privacy rights and choices of the device: team@makenotion.com.

Below is a summary of key points:

Data handling

Notion is dedicated to developing and implementing data privacy processes and safeguards that meet industry standards and best practices. Notion conducts ongoing training for their teams to ensure that they are up to speed with developments in legislation and essential privacy and security practices. Every Notion employee and contractor signs up to non-disclosure terms to maintain the confidentiality and security of your data. Notion also holds any vendors that handle personal data to the same data management, security, and privacy practices and standards to which we hold ourselves.

Agreements

Notion strives to keep all of their agreements up to date with the latest regulations and industry standards. Their Master Subscription Agreement and Data Processing Addendum describe in detail Notion's data privacy processes, standards, safeguards and our compliance with data protection legislation. To ensure that their terms track with the GDPR, CCPA and other global privacy standards they continually have their terms assessed by leading privacy experts in multiple jurisdictions.

Data governance

Data governance relates to the policies and procedures that dictate how data is procured and used throughout its life cycle. From creation and collection to processing, distribution, storage and deletion. Notion's commitment to data governance is key to keeping their users data secure, private, accurate, and accessible.

Policies

Notion seeks to be as transparent as possible with customers about how they collect, process, store, and use their personal data. In order to achieve this Notion maintains comprehensive and detailed policies regarding how they handle personal information. These policies describe in detail how users can exercise their rights with regard to their data.

[2] https://www.notion.so/GDPR-c8eac6ea83a64fb1a3ea3bcd5c3d4951

GDPR

The General Data Protection Regulation (GDPR) is a comprehensive data protection law that governs the collection of and use of personal data of EU residents, and that allows data subjects to exercise control over their data. As the GDPR is widely considered to be the most stringent global privacy standard, Notion has mapped their privacy program to the GDPR and other global privacy regulations.

2.2.3 Visibility of EU Funding and disclaimer

In accordance with the obligations regarding the dissemination of results, as stated in the Grant Agreement, all project materials produced in the context of the project (publications, website, flyer etc.) must acknowledge EU funding and should be accompanied by the EU emblem and the following text: *"This project has received funding from the* European Union's HORIZON-EIC-2022-PATHFINDERCHALLENGES-01 programme under Grant Agreement N° 101114899".

The Grant Agreement also states that "*any dissemination of results must indicate that it reflects only the author's view and that the Agency is not responsible for any use that may be made of the information it contains*". The following disclaimer will be used in all Veriqub dissemination materials:

"The content of this publication is the sole responsibility of the Veriqub consortium and can in no way be taken to reflect the views of the European Commission. The European Commission is not responsible for any use that may be made of the information it contains."

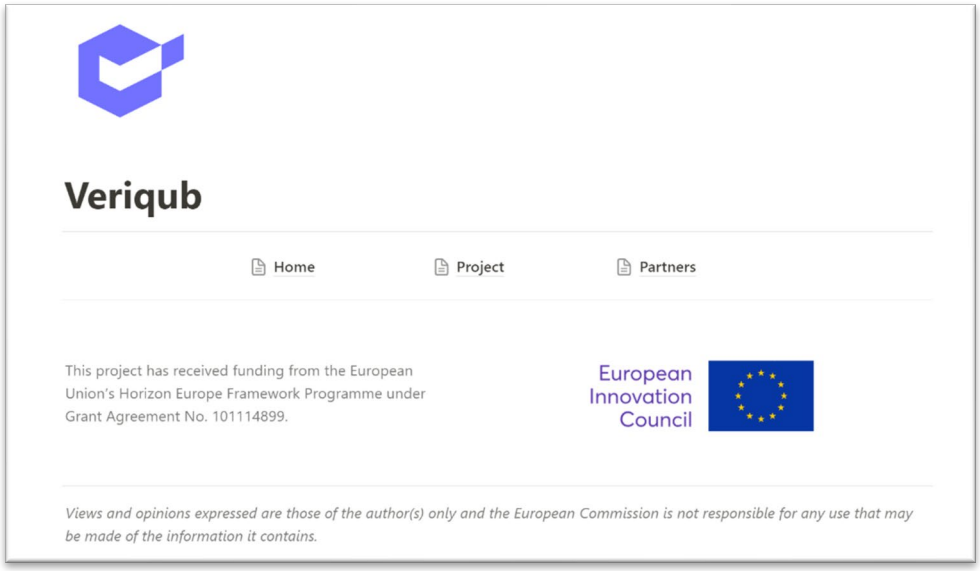

FIGURE 15 WEBSITE EU DISCLAIMER

Annex 1. Notion Data Processing Addendum

(Deprecated February 22, 2023)

This Data Processing Addendum ("**DPA**") forms part of the Master Subscription Agreement (the "**Agreement**") between Customer and Notion.

1. Subject Matter and Duration

1.1 Subject Matter. This DPA is intended to govern Customer's provision and Notion's Processing of Customer Personal Data pursuant to the Agreement. All capitalized terms that are not expressly defined in this DPA will have the meanings given to them in the Agreement. If and to the extent language in this DPA or any of its attachment's conflicts with the Agreement, this DPA shall control.

1.2 Duration and Survival. This DPA will become binding upon the effective date of the Agreement and shall survive until expiration or termination of the Agreement or the return or deletion of Customer Personal Data in accordance with Section 8.1, whichever later.

2. Definitions

For the purposes of this DPA, the following terms and those defined within the body of this DPA apply.

"Controller" means the person who, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

"Customer Personal Data" means Customer Data that is "personal data" or "personal information" under applicable Data Protection Law.

"Data Protection Law(s)" means all worldwide data protection and privacy laws and regulations applicable to Customer Personal Data, including, where applicable, EU/UK Data Protection Law and the California Consumer Privacy Act of 2018 ("CCPA"), as amended from time to time, including any related regulations and guidance provided or issued by the California Attorney General pertaining to same. For the avoidance of doubt, if Notion's processing activities involving Customer Personal Data are not within the scope of a Data Protection Law, such law is not applicable for purposes of this Agreement.

"EEA" means the European Economic Area.

"EU/UK Data Protection Law" means: (i) Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the Processing of Personal Data and on the free movement of such data (General Data Protection Regulation) (the "EU GDPR"); (ii) the GDPR as saved into United Kingdom law by virtue of section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 and the UK Data Protection Act 2018 (collectively, the "UK GDPR"); (iii) the EU e-Privacy Directive (Directive 2002/58/EC); and (iv) any and all applicable national data protection laws made under, pursuant to or that apply in conjunction with any of (i), (ii) or (iii); in each case as may be amended or superseded from time to time;

"Notion Security Standards" means Notion's security standards, as updated from time to time, available at: https://www.notion.so/help/security-and-privacy.

"Process" or "Processing" means any operation or set of operations which is performed on Customer Personal Data or sets of Customer Personal Data, whether or not by automated means, such as

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

“Processor” means the person who, alone or jointly with others, Processes Personal Data on behalf of the Controller;

"Restricted Transfer" means: (i) where the EU GDPR applies, a transfer of Personal Data from the EEA to a country outside of the EEA which is not subject to an adequacy determination by the European Commission; and (ii) where the UK GDPR applies, a transfer of Personal Data from the United Kingdom to any other country which is not subject based on adequacy regulations pursuant to Section 17A of the United Kingdom Data Protection Act 2018, in case whether such transfer is direct or via onward transfer.

"SCCs" means: (i) where the EU GDPR applies, the contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council ("EU SCCs"); and (ii) where the UK GDPR applies, standard data protection clauses for processors adopted pursuant to Article 46(2)(c) or (d) of the UK GDPR ("UK SCCs").

“Security Incident(s)” means any unauthorized or unlawful breach of security leading to, or reasonably believed to have led to, the accidental or unlawful destruction loss, alteration, unauthorized disclosure or access to any Customer Data processed under or in connection with the Agreement, including but not limited to Customer Personal Data.

“Subprocessor(s)” means a third party engaged by Notion to Process Customer Personal Data under the Agreement.

3. Data Use and Processing

3.1 Documented Instructions. The parties acknowledge and agree that Customer is the Controller of Customer Personal Data and Notion is the Processor of such Customer Personal Data. Notion shall Process Customer Personal Data as a service provider strictly for the business purpose(s) agreed between the parties and as provided under the Agreement, this DPA, and any instructions expressly agreed upon by the parties in writing (together, the "Business Purpose"). Customer will not instruct Notion to Process Customer Personal Data in violation of applicable law (including Data Protection Laws). Notion has no obligation to monitor the compliance of Customer’s use of the Services with applicable law (including Data Protection Laws). However, Notion will, unless legally prohibited from doing so, (i) inform Customer in writing if it reasonably believes that there is a conflict between Customer’s instructions and applicable law (including Data Protection Laws) or otherwise seeks to Process Customer Personal Data in a manner that is inconsistent with Customer’s instructions, and (ii) in such event, cease all Processing of the affected Customer Personal Data (other than merely storing and maintaining the security of the affected Customer Personal Data) until such time as Customer issues new instructions with which Notion is able to comply. If this provision is invoked, Notion will not be liable to Customer under the Agreement for failure to perform the Services until such time as the parties agree on new instructions.

3.2 Service provider certification. Notion shall not: (a) sell the Customer Personal Data; (b) retain, use, or disclose Customer Personal Data for any purpose other than for the Business Purpose, including to retain, use, or disclose the personal information for a commercial purpose other than performing its services

under the Agreement; (c) retain, use, or disclose the Customer Personal Data outside of the direct business relationship between Customer and Notion. Notion certifies that it understands the restrictions set out in this Section 3.2 and will comply with them.

3.3 Authorization to Use Subprocessors. To the extent necessary to fulfill Notion's contractual obligations under the Agreement, Customer hereby authorizes Notion to engage Subprocessors. A current list of Notion's Subprocessors can be found in the Notion Security Standards. Customer acknowledges and agrees that Notion's use of such Subprocessors satisfies the requirements of this DPA.

3.4 Notion and Subprocessor Compliance. Notion agrees to (i) enter into a written agreement with Subprocessors regarding such Subprocessors' Processing of Customer Personal Data that imposes on such Subprocessors data protection requirements for Customer Personal Data that are consistent with this DPA; and (ii) remain responsible to Customer for Notion's Subprocessors' failure to perform their obligations with respect to the Processing of Customer Personal Data.

3.5 Notice of and Right to Object to New Subprocessors. Customer may sign up to receive notification of new Subprocessors by e-mailing team@makenotion.com with the subject "Subscribe to New Subprocessors." Once Customer has signed up to receive new Subprocessor notifications, Notion will then provide Customer with notice of any new Subprocessor before authorizing such new Subprocessor to Process Customer Personal Data and allow Customer ten (10) days to submit a legitimate, good-faith objection to such new Subprocessor(s) from Customer's receipt of Notion' notice. In the objection, Customer shall explain its reasonable grounds for such objection. In the event of such objection, the parties will work together in good faith to resolve the grounds for the objection. If the parties are unable to resolve the objection within a reasonable time period, which shall not exceed thirty (30) days, either party may terminate the Agreement by providing written notice to the other party. Notion may replace a Subprocessor if the need for the change is urgent and necessary to provide the Services. In such instance, Notion shall notify Customer of the replacement as soon as reasonably practicable, and Customer shall retain the right to object to the replacement Subprocessor.

3.6 Confidentiality. Notion will ensure that any person whom Notion authorizes to Process Customer Personal Data on its behalf is subject to confidentiality obligations in respect of that Customer Personal Data.

3.7 Customer Personal Data Inquiries and Requests. To the extent Customer, in Customer's use of the Services, does not have the ability to address a request from a data subject exercising their rights under applicable Data Protection Laws (e.g., access, deletion, etc.), Notion shall, upon Customer's request, use commercially reasonable efforts to assist Customer in responding to such data subject request. If a request relating to Customer Personal Data is sent directly to Notion, Notion shall use commercially reasonable efforts to promptly notify Customer within five (5) days of receiving such request and shall not respond to the request unless Customer has authorized Notion to do so. To the extent legally permitted, Customer shall be responsible for any non-negligible costs arising from Notion's provision of assistance under this Section. Customer acknowledges that Notion is reliant on Customer for direction as to the extent to which Notion is entitled to Process Customer Personal Data on behalf of Customer in performance of the Services. Consequently, Notion will not be liable under the Agreement for any claim brought by a data subject arising from any action or omission by Notion, to the extent that such action or omission resulted from Customer's instructions or from Customer's failure to comply with its obligations under applicable law.

3.8 Data Protection Impact Assessment and Prior Consultation. Where required by Data Protection Laws, Notion agrees to provide Customer with reasonable assistance, at Customer's expense, solely to the extent that such assistance is necessary and relates to the Processing by Notion of Customer Personal Data where, in Customer's reasonable judgement, Customer is required under the Data Protection Laws to engage in a data protection impact assessment and/or prior consultation with the relevant data protection authorities.

3.9 Limitation on Disclosure of Customer Personal Data. To the extent legally permitted in each case, Notion shall: (i) promptly notify Customer in writing upon receipt of an order, demand, subpoena, warrant, legal demand or other document purporting to request, demand or compel the production of Customer Personal Data to any non-data-subject third party, including, but not limited to the United States government for surveillance and/or other purposes; and (ii) not disclose Customer Personal Data to the third party without providing Customer at least forty-eight (48) hours' notice, so that Customer may, at its own expense, exercise such rights as it may have under applicable laws to prevent, challenge or limit such disclosure to the extent permitted by applicable laws.

4. Cross-Border Transfers of Customer Personal Data

4.1 Cross-Border Transfers of Customer Personal Data. Customer authorizes Notion and its Subprocessors to transfer Customer Personal Data across international borders, including from the EEA, Switzerland, and/or the United Kingdom to the United States.

4.2 Standard Contractual Clauses. The parties agree that, when the transfer of Customer Personal Data from Customer to Notion is a Restricted Transfer, it shall be subject to the appropriate SCCs as follows:

4.2.1. in relation to Customer Personal Data that is protected by the EU GDPR, the EU SCCs will apply completed as follows:

Module Two and Module 3 will apply, as appropriate;

in Clause 7, the optional docking clause will apply;

in Clause 9, Option 2 will apply, and the time period for prior notice of subprocessor changes shall be as set out in Clause 3.5 of this DPA;

in Clause 11, the optional language will not apply;

in Clause 17, Option 1 will apply, and the EU SCCs will be governed by the laws of Ireland;

in Clause 18(b), disputes shall be resolved before the courts of Ireland;

Annex I of the EU SCCs shall be deemed completed with the information set out in Annex I to this DPA; and

Annex II of the EU SCCs shall be deemed completed with the information set out in Annex II to this DPA;

4.2.2. subject to paragraph 4.2.3 below, in relation to Customer Personal Data protected by UK GDPR, the EU SCCs will apply (in accordance with paragraph 4.2.1 above) but with the following modifications:

any references in the EU SCCs to "Directive 95/46/EC" or "Regulation (EU) 2016/679" shall be interpreted as references to the UK GDPR; references to specific Articles of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK GDPR;references to "EU", "Union" and "Member State law" are all replaced with "UK"; Clause 13(a) and Part C of Annex II of the EU SCCs are not used; references to

the "competent supervisory authority" and "competent courts" shall be interpreted as references to the Information Commissioner and the courts of England and Wales;

Clause 17 of the EU SCCs is replaced to state that "The Clauses are governed by the laws of England and Wales" and Clause 18 of the New EU SCCs is replaced to state "Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may bring legal proceeding against the data exporter and/or data importer before the courts of any county in the UK. The Parties agree to submit themselves to the jurisdiction of such courts";

4.2.3. to extent that and for so long as the EU SCCs, as implemented in accordance with paragraphs 4.2.1 and 4.2.3 above and 4.2.4 below, cannot be used to lawfully transfer Customer Personal Data in compliance with the UK GPDR, the UK SCCs shall be incorporated by reference and form an integral part of this DPA and shall apply to transfers of Customer Personal Data governed by the UK GDPR. For the purposes of the UK SCCs:

Appendix 1 of the UK SCCs shall be deemed completed with the information set out in Annex I to this Agreement; and

Appendix 2 of the UK SCCs shall be deemed completed with the information set out in Annex II to this Agreement; and

4.2.4. in the event that any provision of this DPA contradicts the SCCs (directly or indirectly), the SCCs shall prevail.

4.2.5. The parties agree that, in the event where Data Protection Laws no longer allows the lawful transfer of Customer Personal Data to Notion and/or requires an alternative transfer solution that complies with Applicable Privacy Law(s), Notion will make an amendment to this DPA available to Customer to remedy such non-compliance and/or cease processing of Customer Personal Data without penalty.

5. Information Security Program

5.1 Security Measures. Notion shall implement and maintain commercially reasonable administrative, technical, and physical measures designed to protect Customer Personal Data as set forth in the Notion Security Standards. Notion regularly monitors compliance with these measures. Notion will not materially decrease the overall security of the Service during any Subscription Term.

6. Security Incidents.

6.1 Notice. Upon becoming aware of a Security Incident, Notion agrees to provide written notice to Customer within 72 hours. Any such notification is not an acknowledgement of fault or responsibility. Where possible, such notice will include all details known to Notion and required under Data Protection Laws for Customer to comply with Customer's own notification obligations to regulatory authorities or individuals affected by the Security Incident, which may include, as applicable and if known, how the Security Incident occurred, the categories and approximate number of data subjects concerned, and the categories and approximate number of Customer Personal Data records concerned, the likely consequences of the Security Incident, and measures taken or proposed to be taken by Notion to address the Security Incident, including, where appropriate, measures designed to mitigate its possible adverse effects. Notion shall use commercially reasonable efforts to: (i) investigate and identify the cause of such Security Incident; (ii) remedy or mitigate the possible adverse effects of such Security Incidents, and (iii) reduce the likelihood that such Security Incident recurs. Notion will not assess the contents of Customer

Personal Data in order to identify information subject to any specific legal requirements or assess the applicability of any specific privacy, data protection or cybersecurity requirement pertaining to such information. Customer is solely responsible for complying with Security Incident notification requirements applicable to Customer and fulfilling any third-party notification obligations related to any Security Incident, provided that, at Customer's written request and subject to Customer paying Notion's reasonable fees (at then current rates) and expenses, Notion will provide Customer with assistance reasonably necessary to enable Customer to notify relevant security breaches to the competent data protection authorities and/or affected data subjects, if Customer is required to do so under Data Protection Laws.

7. Audits

7.1 Third-Party Audit Reports. Notion obtains the third-party audits set forth in the Notion Security Standards. Upon Customer's request, and subject to the confidentiality obligations set forth in the Agreement and the entry into specific non-disclosure agreements, Notion shall make available to Customer (or Customer's independent, reputable, third-party auditor) information regarding Notion' compliance with the obligations set forth in this DPA by providing Customer with summaries of the most recent third-party audits reports referenced in the Notion Security Standards. All such summaries, to the extent not made generally publicly available by Notion on its website, constitute Notion's Confidential Information.

7.2 Audit of Notion. Where Data Protection Laws afford Customer an audit right, Customer (or Customer's independent, reputable, third-party auditor) may contact Notion in accordance with the "Notices" Section of the Agreement to request an audit of Notion' policies, procedures, and records relevant to the Processing of Customer Personal Data necessary to confirm Notion' compliance with this DPA, provided that the foregoing are within Notion' control and Notion is not precluded from disclosure by applicable law, a duty of confidentiality, or any other obligation owed to a third party. Customer shall reimburse Notion for its costs and expenses, including any time expended in connection with any such audit at Notion' then-current rates, which shall be made available to Customer upon request. Before the commencement of any such audit, Customer and Notion shall mutually agree upon the scope, timing, and duration of the audit, in addition to the reimbursement rate for which Customer shall be responsible. All reimbursement rates shall be reasonable, taking into account the resources expended by Notion. In no event shall Notion be required, in connection with any of its obligations under this DPA or otherwise, to provide information it is precluded from disclosing by applicable law, a duty of confidentiality, or any other obligation owed to a third party. Any audit must be: (i) conducted during Notion' regular business hours; (ii) with reasonable advance notice to Notion; (iii) carried out in a manner that prevents unnecessary disruption to Notion' operations; and (iv) subject to reasonable confidentiality procedures. In addition, any audit shall be limited to once per year, unless an audit is carried out at the direction of a government authority having proper jurisdiction. Customer shall promptly notify Notion of any alleged non-compliance with this DPA discovered during the course of an audit, and Notion shall use commercially reasonable efforts to address any confirmed non-compliance.

8. Data Deletion

8.1 Data Deletion. Upon termination or expiration of the Agreement, Notion shall, upon Customer's request, and subject to the limitations described in the Agreement and the Notion Security Standards, return to Customer (or make available for export in accordance with the Agreement) all Customer

Personal Data in Notion' possession, or securely destroy such Customer Personal Data (excluding any back-up or archival copies which shall be deleted in accordance with Notion' data retention schedule), except where Notion is required to retain copies under applicable laws, in which case Notion will limit its processing of such Customer Personal Data except to the extent required by applicable laws.

9. Processing Details.

9.1 Subject Matter. The subject matter of the Processing is the Services pursuant to the Agreement.

9.2 Duration. Customer Personal Data will be Processed for the duration of the Agreement, including any post-termination retention period specified therein, subject to Section 8.1 of this DPA.

9.3 Categories of Data Subjects. Data subjects whose Customer Personal Data will be Processed pursuant to the Agreement may include Employees, Suppliers, Customers, Job Applicants, Consultants, and/or Contractors.

9.4 Nature and Purpose of the Processing. The purpose of the Processing of Customer Personal Data by Notion is the performance of the Services pursuant to the Agreement.

9.5 Types of Customer Personal Data. Customer represents and warrants to Notion that Customer Personal Data does not and will not contain, and Customer has not and will not otherwise provide or make available to Notion for Processing any sensitive Personal Data, including but not limited to financial information (e.g. credentials to any financial accounts or tax return data); health information (e.g. protected health information subject to the Health Insurance Portability and Accountability Act (HIPAA) or other information regarding an individual's medical history, mental, or physical condition, or medical treatment or diagnosis by a health care professional, health insurance information, or genetic information); biometric information; government IDs or other government-issued identifiers (e.g. social security numbers); passwords for online accounts (other than passwords necessary to access the Services); credit reports or consumer reports; any payment card information or cardholder data subject to the Payment Card Industry Data Security Standard; information subject to the Gramm-Leach-Bliley Act, Fair Credit Reporting Act, or similar laws, or the regulations promulgated thereunder; information subject to restrictions under applicable law governing personal data of children, including, without limitation, all information about children under 16 years of age; or any information that falls within any special categories of data (as defined under the EU/UK Data Protection Law or otherwise interpreted under the implementing laws of the EEA member states).

Annex I - Data Processing Description

This Annex I forms part of the DPA and describes the processing that Notion (as the Processor) will perform on behalf of the Customer (as the Controller).

A. LIST OF PARTIES

Controller(s) / Data exporter(s): [*Identity and contact details of the controller(s) /data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union*]

Name: *Customer listed in the applicable Order Form.*

Address: *Address listed in the applicable Order Form.*

Contact person's name, position and contact details: *Contact person listed in the applicable Order Form.*

Activities relevant to the data transferred under these Clauses: *Processing to carry out the Services pursuant to the Agreement entered into between Customer and Notion.*

Signature and date: *This Annex I shall automatically be deemed executed when Customer agrees to the Agreement.*

Role (controller/processor): *Controller*

Processor(s) / Data importer(s): *[Identity and contact details of the processor(s) /data importer(s), including any contact person with responsibility for data protection*]

Name: *Notion Labs, Inc.*

Address: *2300 Harrison Street, Floor 2, San Francisco, CA 94110 USA*

Contact person's name, position and contact details: *Hasani Caraway, General Counsel, hasani@makenotion.com*

Activities relevant to the data transferred under these Clauses: *Processing to carry out the Services pursuant to the Agreement entered into between Customer and Notion.*

Signature and date: *This Annex I shall automatically be deemed executed when Customer agrees to the Agreement.*

Role (controller/processor): *Processor*

B. DESCRIPTION OF PROCESSING/ TRANSFER

EU SCC Module: *C2P (Module 2)*

Categories of Data Subjects: *The personal data transferred may concern the following categories of data subjects set forth in Section 9.3 of the DPA:*

Employees, Suppliers, Customers, Job Applicants, Consultants, and Contractors

Purpose(s) of the data transfer and further processing/ processing operations: *The purpose of the transfer is the performance of the Services pursuant to the Agreement.*

Categories of Personal Data: *The personal data transferred concern the categories of data as set forth in Section 9.5 of the DPA.*

Sensitive data transferred (if applicable) and applied restrictions or safeguards: *As set forth in Section 9.5 of the DPA, sensitive data are expressly excluded from the scope of the Services.*

Frequency of the transfer: *Continuous*

Nature and subject matter of the processing: *The subject matter of the Processing is the Services pursuant to the Agreement.*

Duration of the processing: *The duration of the data processing under this DPA is until the termination of the Agreement in accordance with its terms.*

Retention period (or, if not possible to determine, the criterial used to determine the period): *As above.*

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance (e.g. in accordance with Clause 13 SCCs):

Where the EU GDPR applies, the Irish Data Protection Commissioner's Office.

Where the UK GDPR applies, the UK Information Commissioner's Office.

Annex II - Technical and Organisational Security Measures

Description of the technical and organisational measures implemented by the Processor(s) / Data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons:

Measures of pseudonymisation and encryption of personal data

Notion encrypts data in transit via TLS 1.2, and at rest using the AES-256 algorithm.

Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services

Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services include:

Access to production systems is regulated through VPN, leveraging unique accounts and role-based access within operational and corporate environments. Authorization requests for access are tracked and logged on a regular basis. Removal of access for employees upon termination or change of role. Multi-factor Authentication (MFA) is required for access to critical and production resources. Strong passwords are required, never stored in clear text and are encrypted in transit and at rest.

Mandatory security training for employees is required, covering data protection, confidentiality, social engineering, password policies and overall security responsibilities. Confidentiality requirements are imposed on employees. NDAs with third parties are required. Separation of networks based on trust levels are in place.

Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

Notion has processes in place to ensure ongoing confidentiality, availability and resilience to customer accounts and personal data and during a security incident to help restore timely access to personal data following an incident.

Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing

Notion performs annual penetration tests for all components of the Services, including web and mobile applications.

Notion maintains security incident management policies and procedures. Notion notifies impacted customers without undue delay of any unauthorized disclosure of their respective Customer Data by Notion or its sub-processors of which Notion becomes aware to the extent permitted by law.

Measures for user identification and authorisation

The Services support SAML for Customers. Access to the Services by Notion personnel is uniquely identifiable, logged and monitored. Access to back-end infrastructure by Notion personnel requires

multiple layers of authentication including requiring unique identifiers, optimal password strength and the use of Multi-factor Authentication.

Measures for the protection of data during transmission

Notion employs TLS 1.2 encryption from the User's browser to the Services, for Customer Data in transit.

Measures for the protection of data during storage

Notion customer instances are logically separated and attempts to access data outside allowed domain boundaries are prevented and logged. Measures are in place to ensure executable uploads, code, or unauthorized actors are not permitted to access unauthorized data - including one customer accessing files of another customer.

Measures for ensuring physical security of locations at which personal data are processed

Subprocessors are responsible for physical security of the data centers and are contractually obligated to ensure that physical security measures and resources are in place. These systems permit only authorized personnel to have access to secure areas. These facilities are designed to withstand adverse weather and other reasonably predictable natural conditions, are secured by around-the-clock guards, two-factor access screening, and escort-controlled access, and are also supported by on-site back-up generators in the event of a power failure. Further information about security provided by AWS is available from the AWS Security Website and the AWS Data Centers Controls Website.

Measures for ensuring events logging

Notion logs authorization requests by personnel to privileged spaces. The application logs user activities including logins, configuration changes, deletions and updates. They are automatically written to audit logs in internal systems. Internal logs capture timestamps, IP addresses, login/logouts, and errors. These logs are only internally available and available for security investigations upon request.

Measures for ensuring system configuration, including default configuration

Notion monitors changes to in-scope systems to ensure they follow processes which align to our Change Management Policy. Changes are tracked in our change management system and managed to ensure that they follow the process to mitigate the risk of undetected changes to the production systems.

Measures for internal IT and IT security governance and management

Notion has internal information security policies and procedures which are communicated to all employees upon hire and at least annually. Notion conducts Information Security training upon hire and at least annually thereafter. The Information Security function reports to the Legal department who is authorized by senior leadership to take necessary actions to establish, implement and manage Notion's Information Security Program.

Measures for certification/assurance of processes and products

Notion is audited annually by a reputable third party to attest that our commitment to controls and safeguards are in place. Currently Notion holds industry standard certifications showing our commitment to safeguard the confidentiality and privacy of information stored and processed on our service.

Measures for ensuring data minimisation

Data is collected and processed in accordance with stated purposes, access is provisioned and restricted in accordance with roles and requirements for job responsibilities.

Measures for ensuring data quality

Notion has a process that allows data subjects to exercise their privacy rights (including a right to amend and update information), as described in Notion's Privacy Policy.

Measures for ensuring limited data retention

Automatic deletion is implemented to enforce data retention limitations. Notion will maintain all terminated customer accounts in an inactive status for up to 30 days and after such period account data are securely overwritten from production within 90 days (up to a max of 180 days). Backup data is deleted within 180 days of account termination.

Measures for ensuring accountability

Notion maintains Records of Processing Activities and performs Privacy Impact Assessments, when applicable, to the Services.

Measures for allowing data portability and ensuring erasure

Notion customers have the ability to export all Customer Data from their Workspace in either HTML, Markdown or PDF format. Notion has a process which allows data subjects to exercise their privacy rights (e.g., right of erasure or right to data portability) as described in Notion's Privacy Policy.

Annex III - UK Addendum

This Annex III forms part of the DPA and applies in accordance with Section 4 ("Cross-Border Transfers of Customer Personal Data") of the DPA.

Start Date: The date of the Agreement.

Parties: Exporter (who sends the Restricted Transfer) ; Importer (who receives the Restricted Transfer)

Parties' details:

Exporter Name: *Customer listed in the applicable Order Form.*

Address: *Address listed in the applicable Order Form.*

Contact person's name, position and contact details: *Contact person listed in the applicable Order Form.*

Importer Name: *Notion entity listed in the applicable Order Form.*

Address: *Notion address listed in the applicable Order Form.*

Contact person's name, position and contact details: Hasani Caraway, General Counsel, hasani@makenotion.com

Addendum EU SCCs: The version of the EU SCCs incorporated to the DPA, including the information provided in Section 4 (Cross-Border Transfers of Customer Personal Data) and the annexes to this DPA, with only the modules, clauses or optional provisions of the approved EU SCCs brought into effect for the purposes of this Addendum as set out in section 4.2.1 of the DPA.

Appendix Information: See Annex I

Ending this Addendum when the Approved Addendum changes: Neither Party

Mandatory Clauses: Part 2: Mandatory Clauses of the UK Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.

Describe the specific technical and organisational measures to be taken by Data Importer to be able to provide assistance to the Data Exporter:

Self-service system for data portability and deletion.

Through the Workspace settings menu, Notion customers are able to export Customer Data from their Workspaces at the page-level or Workspace-level, or request to delete a Workspace.

Last updated: August 4, 2022