PERSONAL DATA PROCESSING AGREEMENT

EFFECTIVE DATE: ________________________

This Data Processing Agreement ("**DPA**") is entered into as of the Effective Date by and between: (1) **Explain Everything sp. z o.o.** a limited partnership established under the laws of the Republic of Poland (member state of the European Union), with its registered office in Kamieniec Wrocławski, Orzechowa Street 4; (2) **Explain Everything Sales, Inc**. established under the laws of the State of New York based in New York, 119 W. 24th Street, NY 10011, USA; (3) **Explain Everything Discover, Inc.** established under the laws of the State of New York, based in New York, 119 W. 24th Street, NY 10011, USA; (4) **Explain Everything, Inc.** established under the laws of the State of New York, based in New York**,** 119 W. 24th Street, NY 10011, USA (together "**Explain Everything**" or simply "**we**") and the entity or person set forth on the last page hereto ("**Customer**" or simply "**you**"). Explain Everything and Customer are sometimes referred to individually as "**Party**" or collectively as "**Parties**".

This DPA is made with reference to the following facts:

(a) the Customer is interested in using Explain Everything application in the business version (the software and associated services are jointly referred to as "**Services**");

(b) the use of the Services requires that some of personal data controlled by the Customer is processed by Explain Everything;

(c) on the basis of Data transfer agreement concluded on May 21st 2018, we are Joint Controllers of data obtained by each entity, thus we will jointly process your data hereunder;

(d) under art. 28 of the 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 ("**GDPR**") before the Customer starts using the Services, a Data Processing Agreement must be concluded between the Customer and Explain Everything.

2. GENERAL

2.1. You, as the data controller, acknowledge and understand that:

(a) you are the controller of all personal data that you have collected and procced in our Service ("**Customer Data**").

(b) making use of the Services requires that we store and synchronize Customer Data with the Services;

2.2. You, as the data controller, confirm that:

(a) this DPA along with the Terms of Use and Privacy Policy of the Services are your complete and final instructions to us for the processing of Customer Data. We will immediately inform you, if in our opinion your instructions may infringe the GDPR or other data protection laws.

(b) Customer Data was and will be obtained in accordance with applicable laws, including the GDPR and that all required consents (if necessary) from people whose personal data are processed using the Services were collected and all information duties fulfilled;

(c) you will not process special categories of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation

2.3. We, as a data processor, undertake:

(a) to only process Customer Data through the Services to make it possible for you to make use of the Services, solely on the basis and under the conditions specified in this DPA and applicable provisions of law;

(b) not to record, register, store, back up, or physically access the content of Customer Emails.

3. SCOPE OF PERSONAL DATA AND CATEGORIES OF DATA SUBJECTS

3.1. Customer Data encompasses the personal data, which you entered into the Service as the controller. These data may include following categories of personal data: [__]. These people are those who will be concerned by this DPA.

3.2. We may process Customer Data only at your explicit request in terms of its: storage, restriction, erasure or destruction.

4. SUBPROCESSING

4.1. We use [_the name of service for example AMS_] to provide our Services to you. This means that Customer Data will be processed by the [_the name of service for example AMS_]. You can find detailed terms and conditions of services provided by [_the name of service for example AMS_] and its affiliates in [_link to the privacy policy of the subprocessor confirmed it is GDPR compliance_]. These documents describe [_the name of service for example AMS_] obligations regarding security of data and measures that were implemented to protect the confidentiality of Customer Data.

4.2. [_subprocessors_]

4.3. You acknowledge and agree that we may use services of the above companies, its affiliates and subcontractors, as described above, as subprocessors to provide the Services to you. These entities may be engaged only within the limits and for the purpose of providing the Services to you. The standard of personal data protection applicable to these subprocessors is at least equal to the protection standard provided by us.

5. COPIES AND DISCLOSURE OF DATA

5.1. We will not create copies or duplicates of any data without your knowledge, except for backup copies concerning the following types of data:

(a) the Services' settings and configuration details;

(b) Customer Data.

5.2. These backup copies are necessary to ensure smooth functioning of the Services. All backup copies are automatically created by Service and stored on [__]. We will not use these backup copies outside of Service environment or for any other purposes than those specified above.

5.3. We will not create backup copies of any other types of data than those specified in point 4.1 above.

5.4. We will not disclose Customer Data to law enforcement unless required by law. If law enforcement contacts us with a request for Customer Data, we will attempt to redirect the law enforcement agency directly to you. If compelled to disclose Customer Data to law enforcement, we will promptly notify you and provide a copy of the demand unless we are legally prohibited from doing so.

6. ASSISTANCE IN FULFILLMENT OF THE RIGHTS OF DATA SUBJECTS

6.1. We will help you fulfill your duty to respond to the requests of data subjects, particularly in relation to the right to be forgotten, the right to data portability, the right to restriction of data processing or the right to object to data processing provided that you inform us immediately of any requests from data subjects that require our assistance. In any event, you should inform us of any requests that you received no later than 3 (three) business days from its receipt. You can do it using this form .

6.2. We have the right to refuse your request if it is forwarded to us later than 3 (three) business days from its receipt by you and if the request is difficult or impossible to fulfill. A request may be difficult or impossible to fulfill especially when it is too complex, evidently unjustified, excessive or impossible to fulfill because of technical limitations.

6.3. We will confirm the receipt of your request within 3 (three) business days from its receipt. Within the next 10 (ten) business days we will let you know if we are able to assist you and we will inform you of the expected deadline to fulfill your request. In any event, the deadline may not be shorter than 2 (two) weeks.

6.4. If we receive a request from your data subject to exercise one or more of its rights under the GDPR, we will redirect the data subject to make its request directly to you.

7. SECURITY

7.1. Considering the risk of violation of the rights and freedoms of individuals and the state of technical knowledge, implementation costs, scope, nature, context and purposes of processing personal data, we declare that in accordance with art. 32 of the GDPR, we have implemented appropriate technical and organizational measures to secure the processing of Customer Data. These measures are described in Appendix 1 to this DPA.

7.2. We undertake to protect Customer Data from unauthorized access, unauthorized removal, damage or destruction and we will take all necessary steps to keep personal data confidential and to protect it in accordance with the provisions of the GDPR.

7.3. We declare that all our employees who are authorized to process personal data, are bound to confidentiality and undergo regular trainings regarding data protection provisions relevant to their work.

7.4. We regularly monitor all internal processes and the technical and organizational measures to ensure that processing is conducted in accordance with the requirements of applicable data protection law and the protection of the rights of the data subject.

7.5. We are entitled to implement alternative, suitable measures than those described in this section above and in Appendix 1 to this DPA, especially due to technical advances and developments. Such measures must not fall below the security level of those described above. We will provide you with an up-to-date version of Appendix 1 anytime you request us to do so during the term of this DPA.

8. DATA BREACHES

8.1. We will notify you without undue delay after becoming aware of a personal data breach. Such notice will, at a minimum:

(a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned, and the categories and approximate number of personal records concerned;

(b) communicate the name and contact where more information can be obtained;

(c) describe the likely consequences of the personal data breach; and

(d) describe the measures taken or proposed to be taken by you to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

9. PERIOD OF PROCESSING AND RETURN OF DATA

9.1. You acknowledge and understand that we will start the processing of Customer Data after you entered Customer Data into Service.

9.2. We will process personal data that you entrust to us for the duration of your subscription for the Services.

9.3. If your subscription of Service is terminated or expires, we will erase Customer Data from the Services within 180 days after you cancel your subscription with us, unless the law requires that this data is processed for a longer period.

9.4. After termination or expiration of your license we will not perform any operations on Customer Data, except for storing it within the Services, unless we are required to do otherwise by law.

10. AUDITING RIGHTS OF THE CUSTOMER

10.1. If you need any additional information regarding how we process and protect Customer Data and fulfill obligations arising out of the GDPR you can contact us at any time using this form .

10.2. You can also verify security measures implemented by our subprocessors and its affiliates by referencing to their Services Terms.

10.3. Starting from June 2018, once every year we will undergo a data security audit regarding the way we process and secure Customer Data. Each audit will result in generation of an audit report ("**Explain Everything Security Audit Report**"). These audits will be conducted by external auditors. Explain Everything Security Audit Report will clearly disclose any material findings by the auditor. We will promptly remediate issues raised in any Explain Everything Audit Report to the satisfaction of the auditor.

10.4. If you request us to do so, we will provide you with a summary of the latest Explain Everything Security Audit Report so that you can verify our compliance with the security obligations under this DPA. This report will be subject to non-disclosure and distribution limitations of Explain Everything and the auditor. You may be requested to sign an additional Non-Disclosure Agreement with us prior to making the summary available to you.

11. CONTROL AND AUDITS

11.1. You should inform us without undue delay of any control or audit performed by competent supervisory authorities if it relates to Customer Data.

11.2. We will inform you immediately of any inspections and measures conducted by the supervisory authorities if they relate to the Services or Customer Data.

12. MISCELLANEOUS

12.1. This DPA can only be modified by a written document signed by both you and us.

12.2. This DPA should be read and construed together with Explain Everything's *Terms and Conditions of Sales and Services*. In case the provisions of Explain Everything's Terms and Conditions of Sales and Services are contrary to the provisions of this DPA, this DPA should prevail.

12.3. This DPA will be governed by the GDPR and the laws of the Republic of Poland, excluding any conflict of law rules. Any and all disputes relating to this DPA will be settled between you and Explain Everything through good faith negotiations. In case these negotiations are not successful, any subsequent dispute should be litigated in front of the competent courts of the Republic of Poland.

12.4. Should any provision of this DPA be found invalid or unenforceable by a court of competent jurisdiction, the rest of this DPA will remain in full effect.

12.5. This DPA can be signed in one or more counterparts and each counterpart will be considered an original DPA. All of the counterparts will be considered one document and become a binding agreement when one or more counterparts have been signed by each of the Parties and delivered to the other.

12.6. The term of this DPA corresponds with the Terms of Use of the Service.

CUSTOMER’S SIGNATURE

Customer Legal Name: ____

Signed:	____
Name:	____
Title:	____

Email: ____

Date: ____

EXPLAIN EVERYTHING’S SIGNATURES

Explain Everything sp. z o.o.

Signed: ____

Name: ____

Title: ____

Date: ____

Explain Everything Sales, Inc.

Signed: ____

Name: ____

Title: ____

Date: ____

Explain Everything Discover, Inc.

Signed: ______________________________________

Name: ______________________________________

Title: ______________________________________

Date: ______________________________________

Explain Everything, Inc.

Signed: ______________________________________

Name: ______________________________________

Title: ______________________________________

Date: ______________________________________

APPENDIX 1 - SUMMARY OF SECURITY MEASURES IMPLEMENTED BY EXPLAIN EVERYTHING

This document describes security measures that we have implemented to ensure that Customer Data is processed in accordance with the law and the DPA. This document is regularly updated to reflect changes made in our security and data privacy compliance program.

1. GENERAL ORGANIZATIONAL MEASURES

(a) **Data Security Officer and Compliance Program**. We have appointed at least one Data Security Officer who is responsible for coordinating, monitoring and improving our security and data privacy compliance program ("**Compliance Program**"). Compliance Program defines clear roles and responsibilities of our personnel. Data Security Officer is responsible for coordinating, monitoring and improving the Compliance Program;

(b) **External audits**. Starting from June 2018, once every year we will undergo a data security audit with regard to the way we process and secure Customer Data. These audits will be conducted by external auditors.

(c) **Confidentiality**. Our entire personnel are subject to confidentiality obligations and may only access personal data subject to a prior, written authorization issued by Explain Everything.

2. TRAINING AND AWARENESS

(a) **Personnel Training**. We conduct regular training sessions for our personnel on data protection rules and personnel roles within our Compliance Program. We also inform our personnel about possible consequences of non-compliance. These training sessions are conducted using anonymized data.

3. PHYSICAL AND ENVIRONMENTAL SECURITY

(a) **Physical Access to Datacenters**. Customer Data is processed within datacenters of the [__]. Access to these datacenters is restricted only to identified [__] staff members. Our personnel may not physically access these centers.

(b) **Physical Access to our facilities**. Only identified and authorized members of our personnel may access our facilities. Unauthorized personnel may not access these facilities.

(c) **Monitoring of Facilities.** Our facilities are constantly monitored by us and external security service to prevent unauthorized access. Visitors may only access a designated space of our facilities where no data is processed.

(d) **Protection from Disruptions**. We use a variety of industry accepted solutions to protect against loss of data due to power supply failure, fire, natural disaster or line interference.

(e) **Component Disposal.** We use industry accepted solutions to delete Customer Data when it is no longer needed.

4. ACCESS CONTROL

(a) **Access Authorization.** We maintain a record of personnel authorized to access our facilities and information systems. We have implemented a system of controls to make sure that no one can stop working for our organization without having their authentication credentials deactivated and all access rights revoked. Additionally, we conduct regular (at least once every 6 months) audits to make sure that authentication credentials that have not been used are deactivated. De-activated or expired identifiers are not granted to other or new members of our personnel. We maintain industry standard procedures to deactivate passwords that have been corrupted or inadvertently disclosed.

(b) **Limitation of privileges.** Only a small, selected group of personnel may grant, alter or cancel access privileges to our facilities and information systems. The scope of access rights granted to our personnel is limited strictly to assets necessary to perform their functions.

(c) **Authentication of users.** We use industry accepted solutions, such as multifactor authentication, to identify and authenticate users who access our IT systems. Passwords are renewed regularly and must comply with minimum requirements imposed by our security policies. We use various best practices designed to maintain the confidentiality and integrity of passwords when they are assigned, distributed and stored.

(d) **Monitoring**. We monitor our information systems against all attempts of unauthorized access and use of expired or invalid credentials.

5. ASSET AND OPERATIONS MANAGEMENT

(a) **Endpoint protection.** All computing endpoints are encrypted and protected against malware._

(b) **Backup copies.** We make regular copies of Services' settings and configuration details and Customer Data.

(c) **Access to backups.** All backups are automatically created by [__] and stored on [__]. We have processes in place which ensure that access to backup copies is restricted to necessary minimum, that backups may not be used outside of [__] environment and that no data can be restored without authorization of senior personnel members.

(d) **Integrity and Confidentiality.** Our personnel have to disable all sessions when leaving our facilities or leaving computers unattended. Only a small, selected group of our personnel who require remote access due to the character of their duties may carry mobile devices and use them outside of our premises. All mobile devices are password protected and have encrypted storage.

(e) **Printing and portable data carriers.** We have procedures in place which guarantee that no data can be printed or copied to portable data carriers without our prior authorization. Members of our personnel are prohibited from using unauthorized portable data carriers within our premises.

(f) **Network controls.** Only authorized devices may use our networks. We have controls in place which ensure that unauthorized devices may not be used within our network.

6. INCIDENT MANAGEMENT

(a) **Malicious Software.** We have anti-malware controls in place to help avoid malicious software gaining unauthorized access to Customer data and our information systems, including malicious software originating from public networks.

(b) **Incident record.** We maintain a record of security incidents which include the date and time of the incident, the consequences of the breach and measures implemented to avoid similar situations in the future.

(c) **Service Monitoring**. We verify and monitor logs against irregularities and suspicious activity.

7. APPLICATION CONTROLS

(a) **Documentation.** We maintain documentation which describes architecture and features of our Service.

(b) **Guidelines and policies.** We maintain guidelines and policies for developers which ensure that personal data processing principles such as privacy by design and privacy by default principles are observed while developing our applications.

(c) **Code review and patch management.** We regularly review application codes for errors and issue patches or fixes.