

Customerly - Data Processing Agreement

This agreement for the protection of personal data is concluded between the Supplier, as defined below, and the customer who accepts this agreement. **"Supplier"** means Clustomerly Limited, with registered office at Accountantonline, Colab Centre, Port Road, Letterkenny, Co Donegal, Ireland and the subject indicated in the Contract as a customer (hereinafter the **"Customer"**) (each a "Party" and together, the "Parties").

GIVEN THAT

The Parties intend to regulate in this agreement for the processing of personal data (hereinafter "DPA" or "Agreement") the terms and conditions of treatment. The responsibility of the services and responsibilities is the responsibility of the processing of personal data pursuant to art. . 28 of the European General Data Protection Regulation of 27 April 2016 n. 679 (hereafter "GDPR");

DEFINITIONS AND INTERPRETATION

1. DEFINITIONS AND INTERPRETATION

1.1. The premises are an integral part of this Agreement. In the Agreement the following terms and expressions will have the meaning associated with them below:

"Effective Date of the Agreement" means the date on which the Client signs or accepts the present Agreement;

"Personal Data" has the meaning of the Legislation on Personal Data Protection and will include, but not limited to, all data provided, stored, sent, received or otherwise processed, or created by the Customer, or by the End User in relation to the use of the Services, to the extent that they are processed by the Supplier, on the basis of the Contract;

"Decision of Adequacy" means a decision of the European Commission on the basis of Article 45 (3) of the GDPR on the fact that the laws of a certain country guarantee an adequate level of protection, as required by the Law on Data Protection personal;

"Notification email" means the address (or addresses) email provided by the Customer, at the time the Service is signed or provided through another official channel to the Supplier, to which the Customer intends to receive notifications from the Supplier ;

"Instructions" means the written instructions given by the Owner in this Agreement (including the related DPA - Special Conditions) and, possibly, in the Contract;

"Legislation concerning the Protection of Personal Data" means the GDPR, and any further regulations and / or implementing regulations issued pursuant to the GDPR or in any

case in force in Ireland concerning the protection of Personal Data, as well as any binding provision that is issued by the supervisory authorities responsible for the protection of Personal Data (eg, the Guarantor for the protection of personal data) and retains binding force (including the requirements of the General Authorizations for the processing of sensitive and judicial data, if applicable and where they maintain their binding effect after 25 May 2018).

"Supplier Personnel" means executives, employee consultants, and other Supplier personnel, excluding the personnel of the Additional Managers of the Treatment;

"Request" means a request for access by a Data Subject, a request for the deletion or correction of Personal Data, or a request for the exercise of one of the other rights envisaged by the GDPR;

"Responsible for further processing" means any subcontractor to whom the Supplier has subcontracted any of the obligations assumed by contract and which, in fulfilling these obligations, may have to collect, access, receive, store or otherwise process Personal Data;

"Service / s" means the service or services covered by the Contracts signed time by time between the Customer and the Supplier;

"End User" means any end user of the Service, Holder of the Treatment;

"Violation of Personal Data Security" means a security breach that involves unintentionally or unlawfully the destruction, loss, modification, unauthorized disclosure or access to Personal Data occurred on systems managed by the Supplier or otherwise on which the Supplier has a control.

1.2. For the purposes of this Agreement, the terms "Interested", "Processing", "Data Controller", "Data Processor", "Transfer" and "Appropriate Technical and Organizational Measures" will be interpreted in accordance with the Protection Law. of Personal Data applicable.

1.3. The terms "including" and "included" will be interpreted as if they were followed by the expression "purely by way of example", so as to provide a non-exhaustive list of examples.

2. ROLE OF THE PARTIES

2.1. The Parties acknowledge and agree that the Supplier acts as the Data Processor in relation to the Personal Data and the Customer acts as the Data Controller of the Personal Data.

2.2. If the Customer carries out processing operations on behalf of another Data Controller, the Customer may act as Data Processor. In this case, the Customer warrants that the instructions given and the activities undertaken in relation to the processing of Personal

Data, including the appointment by the Customer, of the Supplier as further processing Manager resulting from the stipulation of this Agreement has been authorized by the relative Data controller and undertakes to provide the Supplier, upon his simple written request, with the documentation certifying the foregoing.

2.3. Each of the Parties undertakes to comply, in the processing of Personal Data, with the respective obligations deriving from the Legislation regarding the Personal Data Protection applicable.

3. TREATMENT OF PERSONAL DATA

3.1. With the stipulation of this Agreement (inclusive of each DPA - applicable Special Conditions), the Customer entrusts the Supplier with the task of processing Personal Data for the purpose of providing the Services.

3.2. The Supplier undertakes to comply with the Instructions, provided that, if the Customer requests variations with respect to the initial Instructions, the Supplier will evaluate the feasibility aspects and will agree with the Client the aforementioned variations and related costs.

3.3. In the cases referred to in art. 1.2 and in case of requests of the Customer that involve the processing of Personal Data which, in the opinion of the Supplier, in violation of the Law on Personal Data Protection, the Supplier is authorized to refrain from executing these Instructions and will promptly inform the client. In such cases, the Customer will be able to evaluate any changes to the Instructions given or contact the Control Authority to verify the lawfulness of the requests made.

4. LIMITATIONS ON THE USE OF PERSONAL DATA

4.1. When processing Personal Data for the purpose of providing the Services, the Supplier undertakes to process the Personal Data:

4.1.1. only to the extent, and in the manner necessary, to provide the Services or to properly fulfill its obligations under the Contract and this Agreement or imposed by law or by a competent supervisory or control body. In this last circumstance the Supplier will inform the Customer by means of a communication sent to the Notification Email;

4.1.2. in accordance with the Customer Instructions.

4.2. The Supplier Personnel who accesses or otherwise processes Personal Data is responsible for processing such data on the basis of appropriate authorizations and has received the necessary training also regarding the processing of personal data. This personnel is also bound by confidentiality obligations and the company Code of Ethics, and must comply with the privacy and personal data protection policies adopted by the Supplier.

5. THIRD PARTY SECURITY

5.1. In cases where the Supplier resorts to Additional Processing Managers for the performance of specific personal data processing activities, the Supplier undertakes to use additional Processing Managers that ensure adequate technical and organizational measures and ensures that access to Personal Data, and the related processing, will be carried out exclusively within the limits of what is necessary for the provision of the subcontracted services;

6. SECURITY PROVISIONS

6.1. *SUPPLIER'S SAFETY MEASURES* - When processing Personal Data for the purpose of providing the Services, the Supplier undertakes to adopt appropriate technical and organizational measures to prevent unlawful or unauthorized processing, accidental or illicit destruction, damage, accidental loss, alteration and unauthorized disclosure of, or access to, Personal Data, as described below:

Organizational security measures

User Policy and Disciplinary - The Supplier applies detailed policies and regulations, to which all users with access to information systems have an obligation to comply and are aimed at ensuring appropriate behavior to ensure compliance with the principles of confidentiality, availability and integrity data in the use of IT resources.

Authorization of logical access - the Supplier defines the access profiles in compliance with the least privilege necessary for the execution of the assigned tasks. Authorization profiles are identified and configured before the start of treatment, so as to limit access to the data necessary for processing operations.

These profiles are subject to periodic checks aimed at verifying the existence of the conditions for the conservation of the profiles assigned.

Management of assistance interventions - Assistance interventions are regulated in order to guarantee the execution of the only activities foreseen in the contract and to prevent the excessive processing of personal data whose ownership is held by the Customer or the End User.

Impact Assessment on Data Protection (DPIA) - In compliance with articles 35 and 36 of the GDPR and on the basis of document WP248 - Guidelines on the impact assessment in data protection adopted by the Working Group pursuant to art. 29, the Supplier has prepared its own methodology for the analysis and evaluation of the treatments that, considering the nature, the object, the context and the purposes of the treatment, present a high risk for the rights and liberties of the natural persons to the purpose of proceeding with the evaluation of the impact on the protection of personal data before starting treatment.

Incident Management - The Supplier has implemented a specific Incident Management procedure to ensure the restoration of normal service operations in the shortest possible time, ensuring the maintenance of the best levels of service.

Data Breach - The Supplier has implemented a specific procedure aimed at managing events and incidents with a potential impact on personal data that defines roles and responsibilities, the process of detection (presumed or established), the application of law enforcement actions, the response and containment of the incident / violation as well as the methods by which communications of personal data breaches can be made to the Customer.

	<p><u>Training:</u> The Supplier periodically provides its employees involved in the treatment activities, training courses on the proper management of personal data.</p>
--	--

Technical security measures

Firewall, IDPS - Personal data are protected against the risk of intrusion pursuant to art. 615-quinquies of the Penal Code through Intrusion Detection & Prevention systems kept up-to-date in relation to the best available technologies.

Security of communication lines - As far as they are concerned, secure communication protocols are adopted by the Supplier and in line with what technology makes available.

Protection from malware - The systems are protected against the risk of intrusion and the action of programs by activating suitable updated electronic tools at regular intervals.

Authentication credentials - The systems are configured in such a way as to allow access only to persons with authentication credentials that allow their unambiguous identification. Among these, code associated to a keyword, reserved and known only by the same; authentication device in possession and exclusive use of the user, possibly associated with an identification code or a keyword.

Keyword - With regard to the basic features, that is, the obligation to modify the first access, minimum length, absence of elements easily traceable to the subject, rules of complexity, expiry, history, contextual assessment of robustness, visualization and archiving, the keyword is managed in accordance with best practices. The subjects to whom the credentials are assigned are provided with punctual instructions in relation to the methods to be adopted to ensure their secrecy.

Logging - Systems can be configured in ways that allow access to be traced and, where appropriate, the activities carried out by the various types of users (Administrator, Super User, etc.) protected by appropriate security measures that guarantee their integrity .

Backup & Restore - Appropriate measures are taken to ensure that data access is restored in the event of damage to the data or electronic tools, within certain times compatible with the rights of the data subjects.

If the contractual agreements provide for this, an integrated business continuity plan is used, where necessary, with the disaster recovery plan; they guarantee the availability and access to the systems even in the case of negative events of significant scale that may persist over time.

System Administrators - With regard to all users operating as System Administrators, whose list is kept up-to-date and whose assigned

	<p>functions are appropriately defined in specific appointments, a log management system is managed, aimed at the timely tracking of the activities carried out and to the conservation of such data in an unalterable manner suitable to allow ex post monitoring. The activities of the System Administrators are subjected to verification activities in order to check their compliance with organizational, technical and safety measures with regard to the processing of personal data required by current regulations.</p> <p><u>Data Center</u> - Physical access to the Data Center is restricted to authorized parties only.</p> <p>For details of the security measures adopted with regard to data center services provided by the Additional Managers of the Treatment, as identified in the DPA Special Conditions, please refer to the security measures indicated as described by the same Additional Managers and made available in the relevant institutional sites to the following addresses (or those that will be subsequently made available by the Additional Managers):</p> <p>For the Data Center services provided by Amazon Web Services:</p> <p>https://aws.amazon.com/it/compliance/data-center/controls/</p>
--	---

6.1.2. The Supplier will be able to update and modify the above mentioned Security Measures over time, provided that such updates and modifications can not result in a reduction in the overall level of security of the Services. Such updates and changes will be notified to the Customer by sending notification to the Notification Email.

6.1.3. If the Customer requests to adopt additional security measures with respect to the Security Measures, the Supplier reserves the right to evaluate their feasibility and may apply additional costs to the Customer for such implementation.

6.1.4. The Customer acknowledges and accepts that the Supplier, taking into account the nature of the Personal Data and the information available to the Supplier, will assist the Customer in ensuring compliance with the security obligations set forth in Articles. 32-34 of the GDPR in the following ways:

6.1.4.1. Implementing and keeping updated the Security Measures in accordance with the previous points;

6.1.4.2. If the product allows the integration with third-party applications, the Supplier will not be responsible for the application of the Security Measures relating to the components of third parties or how the product will function as a result of integration by third parties.

6.2. *CUSTOMER SAFETY MEASURES* - Without prejudice to the obligations set out in paragraph 6.1 above by the Supplier, the Customer acknowledges and agrees that, in the use of the Services, the Customer remains solely responsible for the adoption of adequate security measures in relation to the use of the Services by its personnel and those authorized to access such Services.

6.2.1. To this end, the Customer undertakes to use the Services and the functionalities of processing Personal Data in order to guarantee a level of protection appropriate to the actual risk.

6.2.2. The Customer also undertakes to take all appropriate measures to protect the authentication credentials, systems and devices used by the Customer or users at the End User to access the Services, and to perform the backups and backups of Personal Data in order to guarantee the restoration of Personal Data in compliance with the law.

6.2.3. Any obligation or liability on the part of the Supplier regarding the protection of Personal Data that the Customer, or the End User, if applicable, retain or transfer out of the systems used by the Supplier and its Additional Managers of the Treatment (for example, in paper archives, or in their own data centers, as in the case of contracts concerning products installed at the Customer or at the Customer's suppliers).

6.3. *SECURITY VIOLATIONS* - Except in the case of Contracts relating to products installed at the Customer or at the Customer's suppliers for which this point 1.3 does not apply, if the Supplier becomes aware of a Security breach of Personal Data, the same:

6.3.1. will inform the Customer without undue delay by means of communication sent to the notification email;

6.3.2. will take reasonable steps to limit possible damage and security of Personal Data;

6.3.3. will provide to the Customer, as far as possible, a description of the breach of personal data security including the measures taken to avoid or mitigate potential risks and activities recommended by the Supplier to the Customer for the management of security breaches;

6.3.4. will consider confidential information pursuant to the provisions of the Contract, information concerning any Security breaches, related documents, notices and not provide information to third parties, outside the cases strictly necessary for the fulfillment of the obligations of the Customer arising from the Legislation on the Protection of Personal Data without the prior written consent of the Data Controller.

6.4. In the cases referred to in paragraph 1.3 above, it is the sole responsibility of the Customer to fulfill, in the cases provided for by the Legislation concerning the Processing of

Personal Data, the obligations of notification of the Security Violation to third parties (to the Final User if the Customer is a Responsible of the Treatment) and, if the Customer is the Data Controller, the Control Authority and the interested parties.

6.5. It is understood that the notification of a breach of security or the adoption of measures aimed at managing a breach of security does not constitute recognition of breach or liability by the Supplier in relation to said breach of security.

6.6. The Customer must promptly notify the Supplier of any improper use of the account or authentication credentials or any security breaches that he has had knowledge of the Services.

7. LIMITATIONS ON THE TRANSFER OF PERSONAL DATA OUTSIDE THE EUROPEAN ECONOMIC AREA (SEE)

7.1. The Supplier will not transfer Personal Data outside the EEA if not in agreement with the Customer.

8. ASSISTANCE FOR CONFORMITY PURPOSES

8.1. The Supplier will provide assistance to the Customer and will cooperate in the following ways in order to allow the Customer to comply with the obligations established by the Legislation regarding the Protection of Personal Data.

8.2. If the Supplier receives requests or complaints from an Interested Person in relation to the Personal Data, the Supplier will recommend to the Interested Party to contact the Customer or the End User, in the event that the latter is the Data Controller. In such cases, the Supplier will promptly inform the Customer of the receipt of the Request by sending notification Email and will provide the Customer with the information available to it together with a copy of the Request or of the complaint. It is understood that this cooperation activity will be carried out on an exceptional basis, since the management of relations with the interested parties remains excluded from the Services and it is the Customer's responsibility to handle any complaints directly and ensure that the contact point for the exercise of rights on the part of the interested parties is the Customer himself, or the End User if the Data Controller. It will be the responsibility of the Customer, or of the Final User if he / she is the Data Controller, to follow up on such requests or complaints.

8.3. The Supplier will promptly inform the Customer, unless this is prohibited by law, with notice to the E-mail notification of any inspections or requests for information presented by the supervisory authorities and police with respect to profiles concerning the treatment of Personal Data.

8.4. If, for the purpose of evasion of the Requests referred to in the previous points, the Customer needs to receive information from the Supplier about the processing of Personal Data, the Supplier will provide the necessary assistance as far as reasonably possible, provided that such requests are presented with adequate notice.

8.5. The Supplier, taking into account the nature of the Personal Data and the information available to it, will provide reasonable assistance to the Customer in making available useful information to enable the Customer to make impact assessments on the protection of Personal Data in the cases provided by law. In this case the Supplier will make available general information on the basis of the Service, such as the information contained in the Contract, in the present Agreement related to the Services concerned. Any requests for personalized assistance may be subject to payment of a fee by the Customer. It is understood that it is the responsibility and exclusive responsibility of the Customer, or the End User, if the Data Controller, to proceed to the impact assessment based on the characteristics of the processing of Personal Data from the same place in the context of the Services.

8.6. The Supplier undertakes to render Services based on the principles of minimizing treatment (privacy by design & by default), it being understood that it is the exclusive responsibility of the Customer, or the End User, if the Data Controller, to ensure that the processing is carried out concretely respecting these principles and verifying that the technical and organizational measures of a Service meet the compliance requirements of the Company, including the requisites envisaged by the Legislation regarding the protection of personal data.

8.7. The Customer acknowledges that, in the case of requests for the portability of Personal Data submitted by the respective Interested Parties, and only in relation to the Services that generate Personal Data relevant to this purpose, the Supplier will assist the Client by providing the necessary information to extract the requested data in a format compliant with the provisions of the Personal Data Protection Legislation.

8.8. The preceding points 8.5 and 8.7 are not applicable in the case of contracts concerning products installed at the Customer or at the Customer's suppliers.

9. CUSTOMER OBLIGATIONS AND LIMITATIONS

9.1. The Customer undertakes to issue Instructions that comply with the law and to use the Services in compliance with the Legislation on Personal Data Protection and only to process Personal Data that has been collected in accordance with the Legislation on Personal Data Protection.

9.2. The possible processing of Personal Data referred to in Articles 9 and 10 of the GDPR will be allowed only if expressly provided for in this agreement; out of such cases, the eventual treatment of such Personal Data will be allowed only by written agreement between the Parties in accordance with the provisions of point 3.2.

9.3. The Customer undertakes to fulfill all the obligations imposed on the Data Controller (and, in cases where such obligations are the responsibility of the Final User, guarantees that similar obligations are imposed on the End User) by the Legislation in Personal Data Protection, including the disclosure obligations towards the data subjects. The Customer also undertakes to ensure that the processing of Personal Data made through the use of the Services takes place only in the presence of a suitable legal basis.

9.4. If the release of the information and obtaining consent must be made through the product subject of the Contract, the Customer declares to have evaluated the product and that it responds to the needs of the Customer. It is also the responsibility of the Customer to assess whether any forms made available by the Supplier to facilitate the fulfillment of the obligations of disclosure and consent (eg model of privacy policy for Apps or information present in the applications), when available, comply with the Legislation in the matter of Protection of Personal Data and adapt it when deemed appropriate.

9.5. It is also the exclusive responsibility of the Customer to manage the Personal Data in accordance with the requests made by the Interested Parties, and therefore to provide for example any updates, additions, corrections and deletions of Personal Data.

9.6. It is the Customer's responsibility to keep the account linked to the notification email, active and updated.

9.7. The Customer acknowledges that, pursuant to art. 30 of the GDPR, the Supplier is obliged to keep a record of the processing activities carried out on behalf of the Data Controllers (or Data Processors) and to collect for this purpose the identification and contact details of each Data Controller (and / or Responsible) for account of which the Supplier is acting and that such information must be made available to the competent authority upon request. Therefore, when requested, the Customer undertakes to give the Supplier the identification and contact details indicated above with the methods identified by the Supplier over time and to keep this information updated through the same channels.

9.8. The Customer therefore declares that the processing of Personal Data, as described in the Agreements, in this Agreement, is lawful.

10. DURATION

10.1. This Agreement will take effect from the Effective Date of the Agreement and will terminate automatically, on the date of cancellation of all Personal Data by the Supplier, as provided for in this Agreement.

11. PROVISIONS FOR THE RETURN OR CANCELLATION OF PERSONAL DATA

11.1. Upon termination of the Service, for whatever reason, the Supplier will cease all processing of Personal Data and

11.1.1. will delete Personal Data (including any copies) from the Supplier's systems or from those on which it has control within the time limit set forth in the Contract, except in the case where the storage of data by the Supplier is necessary in order to fulfill a provision of Irish or European law;

11.1.2. will destroy any Personal Data held in paper format in its possession, except in the case where the storage of data by the Supplier is necessary for the purposes of compliance with Irish or European laws; is

11.1.3. will keep the Personal Data for the extraction available to the Customer for the period of 12 (twelve) months following the termination of the Contract. During this period, the treatment will be limited only to the conservation aimed at maintaining the Personal Data available to the Customer for the extraction referred to in point 11.2.

11.2. Without prejudice to what is otherwise provided in this Agreement, the Customer acknowledges being able to extract the Personal Data, upon termination of the Service, in the manner agreed in the Contract and agrees that it is his responsibility to provide the total or partial extraction of the Personal Data that he considers useful to keep and that such extraction must be carried out before the expiry of the term referred to in point 11.1.3.

11.3. It is understood that the provisions of points 11.1 and 11.2 do not apply to contracts concerning products installed at the Customer or at the Customer's suppliers. In such cases, it is the Customer's responsibility to extract, within and not later than 30 (thirty) days from the end of the Term of the Contract, the Personal Data that it deems useful to keep; the Customer acknowledges that Personal Data may no longer be accessible after the aforementioned term. In the cases referred to in this point 11.3, the Customer is also responsible for the deletion of Personal Data in compliance with the law.

12. LIABILITY

12.1. Each Party is responsible for the fulfillment of its obligations under this Agreement and the related DPA-Special Conditions and by the Legislation concerning the protection of Personal Data.

12.2. Without prejudice to the mandatory limits of the law, the Supplier will be obliged to indemnify the Customer in the event of violation of this Agreement and / or the related DPA - Special Conditions within the maximum limits agreed in the Contract.

13. MISCELLANEOUS PROVISIONS

13.1. This Agreement supersedes any other agreement, contract or understanding between the Parties with respect to its subject as well as any instruction given in any form by the Customer to the Supplier prior to the date of this Agreement regarding Personal Data processed in connection with the execution of the Contract .

13.2. This Agreement may be modified by the Supplier by giving written notice (including by e-mail or with the aid of computer programs) to the Customer. In this case, the Customer will have the right to withdraw from the Contract by written notice sent to the Supplier by registered mail with acknowledgment of receipt within 15 days from receipt of the Supplier's communication. In the absence of exercise of the right of withdrawal by the Customer, in the terms and in the ways indicated above, the modifications to the present Agreement will be understood by these definitively known and accepted and will become definitively effective and binding.

13.3. In case of conflict between the provisions of this Agreement and the provisions of the Contract for the provision of the Services, or in Client documents not expressly accepted by the Supplier in derogation of this Agreement and / or the respective DPA - Special Conditions, the provisions of this Agreement and in the clauses of the relative DPA - Special Conditions.

Service	Customerly
Supplier	Customerly Limited
Categories of PII (Personally identifiable information)	<p>For the purposes of the provision of the Services under the General Conditions, the Supplier may process the following categories of Personal Data provided, stored, transmitted, or created by the Customer, or by the End User in the context of the use of the Product:</p> <ul style="list-style-type: none"> ● Identification data ● Business data ● Log data in systems and applications <p>The Service does not provide for the treatment of particular categories of data, such as data suitable to reveal the state of health, political opinions, philosophical or religious beliefs contained in the documentation managed by the service in question, or the processing of judicial data (art. 10 of the GDPR). Therefore, the user is invited not to enter / upload data belonging to these categories in the documentation managed by the Service.</p>
Categories of interested	<p>In providing the Services, the Supplier may process Personal Data provided, transmitted, stored, or created by the Customer, or by the End User in the context of the use of the Service resulting from assistance operations in relation to the same Services, relating to the following categories of Interested Parties</p> <ul style="list-style-type: none"> ● Customers / Users natural persons
Place of data retention	<p>Cloud SaaS: the Supplier declares that the servers are located at the AWS data center - Amazon Web Services within the European Union (for further details, refer to https://aws.amazon.com/compliance/data-center/controls/)</p>
Third party providers processing personal data of the Customer / End User in the context of the Service	<p>The Provider may use for processing operations of Personal Data related to the provision of the Services (such as Amazon for data center services as specified above) of selected third-party suppliers that offer guarantees of confidentiality of data.</p>

Signed on behalf of the Controller

Signature

Company

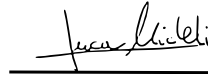
Name

Title

Date

Signed on behalf of the Processor

Signature



Company

Customerly Limited

Name

Luca Micheli

Title

CEO

Date

February 11th, 2021

Please mail this DPA signed at legal@customerly.io