Agreement on the processing of personal data between data processor and sub-processor

Between _____ its registered office in _____ VAT/FISCAL number _____ in person of its duly authorized legal representative on behalf of legal representative hereinafter called Data Processor or simply PROCESSOR, on one side

and

IdWeb S.r.l. its registered office in viale Romagna, 69 – 06012 Città di Castello – PG, P. IVA 02607970544 - REA PG-228909 in person of its duly authorized legal representative on behalf of legal representative hereinafter called Data Sub-Processor or simply SUB-PROCESSOR on the other.

WHEREAS

- a contract was subscribed between parties for the IdSurvey software platform to design and administer CATI CAWI CAPI questionnaires;
- that the Sub-Processor manages the OnCloud platform of IdSurvey software as a service;
- The parties indicate the data controller in the attached table under H. If additional data controllers are identified with subsequent contracts entered into by the manager, the table may be updated and this agreement will extend to them as well.

1. OBJECT OF THE AGREEMENT

This agreement has as content the regulation of the conditions that the Sub-Processor, on behalf of the PROCESSOR, commits to perform data and personal information processing operations as defi ned below.
Within their contractual relationship, the parties commit to respect the current and applicable regulations for personal data processing, in particular the EU REGULATION 2016/679 of the European Parliament and Council of 27th of April 2016, applicable from 25th of May 2018, hereafter referred to as Regulation.

2. DESCRIPTION OF THE PROCESSING LINKED TO THE SUB-PROCESSOR

The Sub-Processor is authorized to process personal data needed for the service(s) supplied on behalf of the Processor.

Nature of the processing operations carried out and type of data

Regarding the nature of the processing operations carried out and the type of data, please note the following:
regarding **personal data whose transmission is implicit in the use of internet communication protocols**. These data are not collected to be associated with

identified subjects, but by their very nature could, through processing and association with data held by third parties, allow users to be identified (e.g. IP addresses). These data are processed for the proper functioning of the website and the services provided and are acquired by computer systems and software procedures during their normal operation.

The Sub-Processor, moreover, although not being ordinarily responsible of operations that imply a comprehension of the applicative domain (data meaning, representation format and functions semantic), in the usual activities the sub-processor is, in many cases, specifically assigned to specific working phases that might involve high findings on data protection. In this cases the Sub-Processor operates as "**System Administrator**" and is obliged to respect applicable *pro tempore* predictions related to the regulations on system administrators included in the Guarantor measure for personal data protection of the 27th of November 2008, measure of the 25th of June 2009.

Typical technical activities of the system administrator, as the data saving (backup/ recovery), the organization of net flows, the management of storing support and hardware maintenance, involve in many case an effective ability to act on information that has to be effectively considered in the same way as a personal data processing; this, also when the administrator doesn't consult the same information "unencrypted".

The actual arrangements cover the regulation of the conditions that the Sub-Processor, on behalf of the Processor, commits to make data and personal information processing operations (in the limited meaning identified above) as follows.

The categories of data that are the object of the processing are therefore represented both by the categories of personal data that the data sub-processor processes in order to render the service, and by those that could be accessible to the Data Sub-Processor during the performance of the services requested.

In particular, as for the first hypothesis, the categories of data processed are summarized in the table below:

Categories of personal data that the Sub-Processor processes in order to render the service.	Tick
Connection data (log or ip)	√
Access credentials	√

As for the second hypothesis, i.e. the types of data that could be accessible to the Data Sub-Processor during the performance of the services requested, the categories of data are those specified below by the Data Processor by ticking the box corresponding to the type of processing:

Types of data that may be accessible to the Sub-Processor during the performance of the services requested.	Tick
General data (Name, Last name, etc.)	√
Particular categories of data (sensitive, biometric and genetic data)	
Data related to automated decisions	

Categories of personal data that the Sub-Processor may access to perform the requested services.	Tick
Identification data (Name, Last name)	
Personal data (birth date, place of birth, address)	
Contact data (phone number, mobile number, email, post address)	
Demographic information (gender, age)	
Identity document data (identity card number or copy)	
Curricula	
Data related to localization	
Other	

When special categories of data are processed to which the Sub-Processor may accidentally access in the performance of services, the Processor must indicate it by ticking the boxes indicated in the table below:

Special categories of personal data to which the Sub-Processor may have access to perform the requested services	Tick
Judicial data related to criminal convictions	
Health related data	
Data revealing racial or ethnic origin	
Data revealing political opinions	
Data that reveal religious or philosophical beliefs	
Data revealing trade union membership	
Genetic data	
Biometric data	
Sexual life related data	
Sexual orientation related data	

Also in order to highlight the presence of vulnerable categories of people, the processor declares that the data concern the following categories of data subjects:_____

_____

3. DURATION OF THE AGREEMENT

The present agreement will have a duration equal to the duration of the service adhered to and described in the introduction. This Agreement shall enter into force between the parties from the signing of both parties, in case of asynchronous signing, at the time of the last signing.

4. OBLIGATIONS OF THE PROCESSOR TOWARDS THE SUB-PROCESSORS

The processors undertakes to:

- to provide the Sub-Processor to personal data processing in n. 2 of this agreement;
- to document in writing all instructions related to data processing by the Sub-Processor;
- to guarantee, from now and for the duration of the processing, the compliance with obligations under the European regulation on data protection by the Sub-Processor;
- to supervise the processing, including the audit implementation and the inspection with the contribution of the Processor.

5. OBLIGATIONS OF THE SUB-PROCESSOR

The Sub-Processor commits in front of the Processor to:

- to treat personal data only for the **scopes** of the processing;
- to treat personal data in accordance with **instructions written** by the Processor, attached to this contract; if the Sub-Processor believes that an instruction received by the Processor represents a violation to the General Regulation on data protection or, to the right of European Union or to the right of a State member, he immediately informs the processing Processor. Moreover, if the Sub-Processor has to proceed to a data transfer to a third country or to an international organization because of the Union right or the right of a State member the sub-processor is under, the sub-processor has to inform the Processor of this juridical duty before the processing unless the right prohibits this information for relevant reasons of public interest;
- to **guarantee the confidentiality** of personal data treated under this contract;
- to guarantee that **people authorized** to process personal data under this contract:
    - commit to comply with privacy or undergo an appropriate legal duty for privacy;
    - receive the needed instructions to maintain personal data protection.
- Take into account, for what concerns tools, products, applications or services, privacy principles from the design (privacy by design) and privacy for default setting (privacy by default).
- the Sub-Processor does not object to a copy of this agreement being sent by the Processor to the Controller, in order to allow the Controller to monitor compliance with the instructions and obligations imposed on the Processor by previous agreement, but it will not be necessary to make available to the Controller the clauses relating to commercial matters which do not affect the legal content of data protection of the agreement with the Sub-Processor.
- the Sub-Processor undertakes that in the event of the failure of the Processor (or other cause resulting in the loss of its capacity to act), the Data Controller shall have the right to order the Sub-Processor to return or erase the personal data that the Processor (and consequently the Sub-Processor) processed on its behalf, in accordance with the provisions set out below regarding the "fate of the data".

6. SUB-PROCESSORS - GENERAL AUTHORIZATION

IdWeb may use another Sub-Processor of processing (from now on called Sub-processor) to perform specific processing activities. In this case IdWeb informs in advance and in writing the Processor of all modifications related to the addition or the replacement of Sub-processors. This information must clearly indicate the processing activities performed by the other Sub-Processor, the identity and contact information of the other Sub-Processor, and the date of the contract related to the sub-processing. The Sub-Processor shall have a period of 15 days from receipt of the information to submit its objections. The sub-processing may not commence until the specified period has expired without the responsible party filing an objection.

IdWeb's Sub-Contractor shall be required to perform its obligations under this Agreement on behalf of and in accordance with the instructions of the Processor. It is IdWeb's responsibility to ensure that the other Sub-Contractor it has identified has the same sufficient guarantees as to

the implementation of the appropriate technical and organizational measures so that the processing meets the requirements of the General Data Protection Regulation.
If the new responsible party (Sub-Contractor) identified by IdWeb fails to fulfill its data protection obligations, IdWeb retains full responsibility to the Responsible Party for fulfilling the obligations of its Sub-Contractor ("Sub-Sub-Contractor").

7. RIGHT OF THE DATA SUBJECTS INTERESTED TO THE REPORT

It's a responsibility of the processor to provide the report to people interested to the processing of the data collected.

8. EXERCISE OF THE RIGHTS OF THE DATA SUBJECTS

The sub-processor has to help the processor (and the Controller on whose behalf the processor operates) as far as possible in fulfilling his duties of providing feedback to data subjects' requests for the access, correction, deletion and opposition right, for the processing restriction, the right to data portability, the right to oppose to an automated personal decision (including profiling).
When the data subjects go to the sub-processor for the exercise of their rights, the sub-processor has to send these requests, as soon as they're received, by email to the email address specified at the end of this agreement (attachment B). When the processor fails to fulfill this task, the sub-processor is free from any obligation.

9. COMMUNICATION OF A PERSONAL DATA BREACH

The Data Sub-Processor communicates to the Data Processor all personal data breach **within a maximum of 48 hours** from the moment he becomes aware of the breach, as follows: communication to the email address specified in the attachment B of this contract.
This communication shall be accompanied by the news of the provision (if possible) of all useful documentation (its transmission has to be agreed by the parties) to allow the Data Processor to legally provide, if needed, the notification of the breach to the supervisory authority.

10. ASSISTANCE TO THE DATA SUB-PROCESSOR FOR THE RESPECT, FROM THE PROCESSOR, OF THE DUTIES OF THE PROCESSOR HIMSELF, PROVIDING INFORMATION IN POSSESSION

The sub-processor helps the processor in the evaluation of the impact on the protection of personal data.

The sub-processor helps the processor in the preventive consultation addressed to the Supervisory authority.

11. SECURITY MEASURES

The sub-processor undertakes, pursuant to Article 32, to apply security measures described in the attachment "IdSurvey OnCloud Infrastructure" that the processor declares as adequate and compliant to the instructions to provide.
The processor delegates to the Sub-Processor the adoption of different measures than those described in the attachment "IdSurvey OnCloud Infrastructure" provided that the sub-processor respects parameters defined in the Article 32 of the Regulation. The processor and the sub-processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

- the pseudonymisation and encryption of personal data;
- measures that can ensure the ongoing confidentiality;
- the integrity, availability and resilience of processing systems and services;
- measures that can restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

Moreover, with regard to processing performed to provide the Service to authorized people with the task of "System Administrator", the Sub-Processor must also respect applicable *pro tempore* previsions related to the regulation on system administrators included in the regulation of the Supervisor for personal data protection of November 27th, 2008 edited according to the regulation of June 25th, 2009.
The Sub-Processor, in particular, commits to define the functions of system administrator only after an assessment of the characteristics of experience, capability and reliability of the designed subject, that has to provide adequate guarantee of the full respect of the actual dispositions on processing, including the profile related to security.
The Sub-Processor also commits to directly and specifically preserve the identification details of individuals appointed as system administrators, and to promptly provide them to the Processor upon his request.
Lastly, the Sub-Processor commits to adopt adequate system for the record of logic login (computer authentication) to processing system and electronic archives of the system administrators. The record (log access) has to have the characteristics of completeness, inalterability and possibility to be verified for their adequate integrity until the achievement of the purpose they're requested for. The record has to include temporal references and the description of the event that generates them and has to be stored for a reasonable period, not less than six months;

12. FATE OF DATA

At the end of the data processing service, the Sub-Processor undertakes to return (by downloading the data directly from the software) all personal data to the Processor, unless the latter instructs him to destroy them.
The return shall be accompanied by the destruction of all copies existing in the Sub-Processor's computer system.

13. DATA PROTECTION SUB-PROCESSOR (DPO OR RPD)

The Sub-Processor is not obliged to appoint a Data Protection Officer (DPO or DPO). However, the Sub-Processor undertakes to inform the Data Processor of the name and contact details of the Data Protection Sub-Processor, should one be appointed.

14. RECORDS OF PROCESSING ACTIVITIES

The Data Sub-Processor declares to keep a written record of all processing activities done on behalf of the processor including all listed elements of the article 30 of the Regulation.

15. DOCUMENTATION

The Data Sub-Processor make needed documentation available to the Data processor to prove the respect of the duties and to allow audit, including inspections, to the Data processor or to any other subject appointed by him, and to contribute to audit.

16. FINAL CLAUSES

The preconditions and the annexes are part of this contract.
This agreement constitutes an exception to the referral made by the "confidentiality and privacy" clauses contained in the IDSURVEY contract and supersedes and replaces in full any act or written or verbal agreement between the parties that regulates the same subject matter and the same object regulated therein.

17. COMPETENT JURISDICTION

All disputes arising from, or in connection with, the subject-matter of this Agreement shall be settled in an amicable way by the Parties. Should this prove impossible, then the Parties hereby agree that the dispute shall be settled by the Tribunal of Perugia-Italy which shall have exclusive jurisdiction.

18. GOVERNING LAW

For anything not expressly provided for in this Contract, the Parties expressly refer to the provisions of Italian law in force at the time of its conclusion that regulate similar cases or similar matters.

Place _____ Date _____

The Processor

_____

The Sub-Processor

_____

Pursuant to and for the effects of Articles 1341 and 1342 the Controller declares to expressly approve clauses n. 17 (competent court) and 18 (applicable law)

Place _____ Date _____

The Processor_____

MANDATE AGREEMENT
for the signing of standard contractual clauses and "additional contractual measures" for the purposes of data transfer to countries outside the EU

At the same time as the agreement on the processing of personal data between data processor and data sub-processor, within the limits defined by the agreement, the parties stipulate, accept and sign, without reservation, this contract of mandate

between _____ its registered office in _____ VAT/FISCAL NUMBER _____ in the person of the legal representative p.t. hereinafter referred to as the data processor, subject with the necessary powers, hereinafter called for brevity DELEGATOR

And

IdWeb S.r.l. with registered office in viale Romagna, 69 - 06012 Città di Castello - PG, P. IVA 02607970544 - REA PG-228909 in the person of the legal representative p.t. below sub-processor for the treatment, subject with the necessary powers, hereinafter referred to for brevity DELEGATE

WHEREAS

The so-called "standard contractual clauses" (or "SCC") are the standard data protection clauses adopted by the Commission which are intended to contractually bind the data importer to the adoption of adequate safeguards on the data transmitted; they therefore replace the GDPR requirements which are not applicable in the country of destination. They are also referred to as model clauses or model clauses. The signing of the SCC represents an adequate guarantee on the basis of which the transfer of personal data, even to countries without legal protection systems comparable to those of the Union, is in any case legally valid (Art. 25(6) dir. 95/46/EC and 46(2)(c) GDPR) .
At present, three different models of clauses are classified as SCC by means of the same number of Commission decisions:

- 2001/497/EC of 15 June 2001 (for transfers between data controllers)
- 2004/915/EC amending Decision 2001/497 as regards the introduction of an alternative set of contractual clauses for the transfer of personal data to third countries (transfers between data controllers)
- 2010/87/EU of February 5, 2010 regarding standard contractual clauses for the transfer of personal data to data controllers established in third countries (controller-sub controller transfers).

Following the ruling known as "Schrems II" made to the Court of Justice of the European Union, standard contract clauses may be accompanied by additional clauses, which offer greater protection to those concerned. These clauses represent the so-called "additional contractual measures".

art. 1 - Object of the mandate

The Data Processor (delegator) acting in the name and on behalf of the Data Controller delegates to the Sub-Processor (delegate) to sign in the name and on behalf of the Controller the standard contractual clauses 2010/87/EU of 5 February 2010 regarding **standard contractual clauses for the transfer of personal data to data processors established in third countries as well as the additional contractual measures that accompany them (data processor - sub processor transfers**) **and without reservation**, its work, where the data sub-processorr, in compliance with the Agreement on the processing of personal data between data processor and data sub-processor, and in particular with the provisions of point 5 of the same agreement, and limited to the service covered by the above mentioned agreement, makes use of a sub-processor that makes it appropriate to transfer the data abroad, in accordance with the provisions of this writing.

art. 2 - Remuneration and charges

For the purposes of the execution of this mandate, no compensation is provided.

art. 3 - Duration of the mandate

This mandate will have the same duration as the Agreement on the processing of personal data between the data processor and data sub-processor, above mentioned.

Place _____ date _____

The Delegator (Data Processor) The Delegate (Data Sub-Processor)

_____ _____

Attachment A

Processor's DPO name (if applicable)	Contact Information

Attachment B - Contact details

Contact details of the Processor for the communications provided for in this agreement

Event	Contact Information
Data Breach	
Access requests	
Supervisor Authority or Other Authority	

Contact details of the Sub-Processor for the communications provided for in this agreement

Event	Contact information
Data Breach	Andrea Martinelli - andrea.martinelli@idweb.it
Access requests	Andrea Martinelli - andrea.martinelli@idweb.it
Guarantor Authority or Other Authority	Andrea Martinelli - andrea.martinelli@idweb.it

Attachment C

"Sub-processors"
The Sub-Processor is authorized to sub-contract part of the processing operations to the following sub-processors (whether or not belonging to the Group of the Processor).

The following table maps the sub-processors hired by the Sub-Processor.

Country where the Processor is established	**Sub-Processor**	**Sub-processors**
_____	Italy	Italy, France, Denmark and the United States.

Sub-processor	**Contact details**	**DPO**
OVH Srl (Socio Unico) Capitale Sociale €. 10.000,00 i.v.– REA n° 1873458.	Headquarter: Via Leopoldo Cicognara, 7 - 20129, Milan - Italy	**Grégory Gitsels** - Data Protection Offcer
The Rocket Science Group , LLC (Mailchimp service)	Headquarter: 675 Ponce de Leon Ave. NE, Atlanta, Georgia 30308, US .	dpo@mailchimp.com
ONLINECITY.IO ApS VAT. no. DK27364276	Buchwaldsgade 50 - 5000 Odense C - Danmark • Tel (+45) 6611 8311 • e-mail tinfo@onlinecity.io	N.A.

Services not provided by the Sub-Processor and subject to separate agreements between the Sub-processor and the Processor are excluded.

The table of sub-processors will be updated from time to time and the Processor will be notified accordingly so that he can oppose the use of new sub-processors.

Attachment D

Model for the communication of data violation from the Sub-Processor to the Processor (for the purposes of the so-called "data breach")

BREACH REPORT

Part 1: Notice of Breach	**To be filled in by the person who discovered the breach**
Date of discovery of the breach:	
Date of the breach:	
Where did the breach occur? Name and description of the database or tool (network computer, laptop, tablet, usb flash drive other removable memory, external disk, file or part of a file, backup tool, paper document or other -specify)	
Location of the device or database:	
Name of the person who discovered the breach:	
Contact details of the person who discovered the breach:	
Short description of the breach: • reading (presumably the data has not been copied); • copying (the data is still present on the processor's systems); • alteration (the data is present on the systems but has been altered); • deletion (the data are no longer on the processorr's systems and neither has the author of the violation); • theft (the data are no longer on the processor's systems and the infringer has them); • other (please specify).	
Number of parties involved: (first approximate estimate; if it is possible to determine it, if it involves all interested parties, specify it; also specify if it is not possible to determine the number and if the number will presumably remain unknown)	
Does the breach pose a risk to those concerned? (describe briefly if you believe it involves a risk)	
Brief description of the actions already taken to mitigate the risk:	

	To be completed by the recipient
Received by:	
Date:	
Next actions (notification communication):	
By:	

Part 2: risk assessment	**To be filled in by the person competent to make the evaluation**
Description of the IT systems, tools, devices of the archives involved in the violation:	
Technical and organizational measures applied to the data:	
Description of the event: • loss; • unavailability; • reading (presumably the data has not been copied); • copy (the data is still present on the processor's systems); • alteration (the data is present on the systems but has been altered); • deletion (the data are no longer on the processor's systems and neither has the author of the violation); • theft (the data are no longer on the processor's systems and the infringer has them); • unauthorized external access; • unauthorized internal access; • error; • natural phenomenon (fire, flood, etc.); • other (please specify).	
What is the nature of the information affected by the violation? (computer copy of paper documents, computer documents, paper documents)	
How many data are involved? E.g. They stole a database with 1000 IP addresses, it is not known how many users they belong to. It is not necessary to specify a number: if a database of medical records is violated, the data will be "many", even if it refers to a few patients. In case of loss or theft of a laptop or other device, when was the last available backup made?	
Is this unique information? Could this violation have legal financial consequences, damage to the image or reputation of the Processor or the Sub-Processor party or other third parties if made known?	
How many people are involved in the violation?	

Are particular categories of data or other high-risk data involved? (indicate the categories involved) Categories: personal data / tax code; access and identification data (user name, password, customer ID, other); • High risk data they reveal: • racial or ethnic origin; • political opinions; • religious or philosophical beliefs; • trade union membership; • data related to health status; • data relating to sexual life or sexual orientation; • genetic data; • biometric data; • data relating to crimes or criminal convictions.	
Type of interested parties: • candidates; • employees; • employees of business partners (e.g. dealers, suppliers, etc.); • customers (including prospects). Attention in particular to: • personal information relating to particularly vulnerable categories or relating to minors; • special information relating to workers, such as aptitude tests, payroll, etc.; • whistleblower.	
Possible consequences: A) physical, material or immaterial damage to individuals (e.g. information that may compromise the safety of those concerned if disclosed); B) identity theft or usurpation (information that can be used to compete identity theft or other crimes such as bank accounts or other financial and identifying information such as copies of identity cards and passports or other identification documents); C) loss of control of personal data concerning data subjects or limitation of their rights; D) discrimination (e.g. data on ethnicity, race, religion, philosophical belief, sexual orientation, sometimes trade union membership); E) financial losses; F) unauthorized pseudonymisation (e.g. whistleblowing); G) damage to reputation; H) loss of confidentiality of personal data protected by professional secrecy; I) any other significant economic or social damage to the individual concerned; J) serious distress and stress if information is disclosed or disseminated; K) information relating to the identity of individuals who have used whistleblowing procedures and cause retaliation jeopardize investigations.	
Is the violation localized or generalized to the entire system?	
Is it possible to overcome the incident that caused the violation with normal restoration operations?	

Alternatively, is the intervention of external parties necessary?	
Is the violation only temporary or is it permanent?	

Part 3: Actions undertaken	**To be completed by the competent person**
Date:	
Entry in the register / no. violation:	
How many personal data records have been affected by the data breach? Indicate approximate number • from 1 to 100; • from 100 to 1000; • from 1000 to 10,000; • from 10,000 to 100,000; • from 100.000 to 500.000; • from 500.000 to 1.000.000; • over 1.000.000;	
Actions taken - What technological and organizational measures have been taken to contain the data breach and prevent similar future breaches?	
What technological and organizational measures have been taken (or are proposed to be taken) to mitigate the possible negative effects of the violation?	
Follow up.	
Notification must be made to the competent territorial authority:	yes/no
It is necessary to give communication to the interested parties:	yes/no (details)
The violation may concern: A) information that may compromise the safety of those concerned if disclosed; B) information that may result in discrimination if disclosed C) information relating to minors or weak individuals; D) information which, if disseminated, is detrimental to reputation; E) information that can cause serious discomfort or stress if disclosed.	

Attachment E

General instructions given by the Data Processor to the Data Sub-Processor

The Sub-Processor, although not exhaustively, will have the tasks and attributions listed below, in addition to the further obligations provided for in the above agreement, and will therefore have to

- to keep a register, as provided for by art. 30 of the GDPR, in electronic format, of all categories of activities related to the processing carried out on behalf of the Company, containing:
    - the name and contact details of the Sub-Processor and the Data Processor and, where applicable, the Data Protection Officer;
    - the categories of processing carried out on behalf of the Data Processor;
    - where applicable, transfers of personal data to a country not belonging to the European Union, including the identification of that country and, for the transfers referred to in the second paragraph of Article 49 of the GDPR, the documentation of adequate guarantees;
    - where possible, a general description of the technical and organizational security measures taken;
- organize the structures, offices and skills necessary and appropriate to ensure the proper performance of the contract;
- refrain from contacting the names processed through the service for purposes other than the assignment;
- not disclose or communicate to third parties the information, including personal data processed to make the Service;
- provide for the identification in writing of the persons authorized to process the data in accordance with the applicable regulations and give them specific and detailed instructions aimed at ensuring full compliance with the provisions of the applicable regulations;
- adopt the technical and organizational security measures provided for in the annex "IdSurvey infrastructure on Cloud";
- **notify the Data Processor of any request or communication from the Guarantor Authority or from the Judicial Authority that may be received by sending a copy of the requests to the e-mail address indicated by the Data Processor in order to jointly agree on the response. The Processor will also be promptly notified of any information transmitted by sub-processor persons in relation to requests for government access by authorities or agencies or services of third countries;**
- maintain a constant update on the legal requirements regarding the processing of personal data, as well as on the technological evolution of security tools and devices, methods of use and related organizational criteria that can be adopted;
- ensure strict compliance with the assignment received, excluding any processing or use of personal data not consistent with the specific processing carried out in fulfillment of the assignment.
- Comply with the instructions given by the controller through the idsurvey control panel, in relation to data downloads (portability), deletion, copying, generation of authentication profiles and permissions, etc., which are understood as "written instructions" within the meaning of this agreement.

ATTACHMENT F
Information about processing carried out abroad

Service	Sub-processor	Third country to which data is transferred	Safeguard measure
Mailchimp	The Rocket Science Group , LLC	USA	SCC in Data Processing Addendum

With regard to the provisions of point 5 of the **Agreement on the processing of personal data between Data Processor and Data Sub-Processor, the Data Processor shall be deemed to have been informed of the transfers made in third countries as described in this Attachment**.

ATTACHMENT G
IdSurvey OnCloud infrastructure

For 20 years we have been hosting customer data with the utmost attention to their protection. To ensure the highest possible degree of security, we use effective devices and adopt a range of best practices at all levels of our organization and infrastructure.

Security systems:

- Physical access to servers limited to accredited employees.
- Access to data centers allowed only by badge.
- Video and human surveillance 24/7.
- Rooms equipped with smoke particle detection systems.
- Technical staff present 24 hours on 24, 7 days on 7.
- Generator sets with 48 hours of autonomy.

Our Cloud is based on VMware Enterprise PLUS and is located inside the European community (France).
On request we can also activate the service in other countries outside the EU.

Features of each physical server	
RAM	384 GB ECC
Processor	2 x Intel Xeon Gold 6226R
Core/Thread	32/64
Frequency	2.9 GHz
Disk	2 x 2Tb SSD
Connectivity	4x 10 Gbps
Uptime	99.99%
Connession	4x 10 Gbps

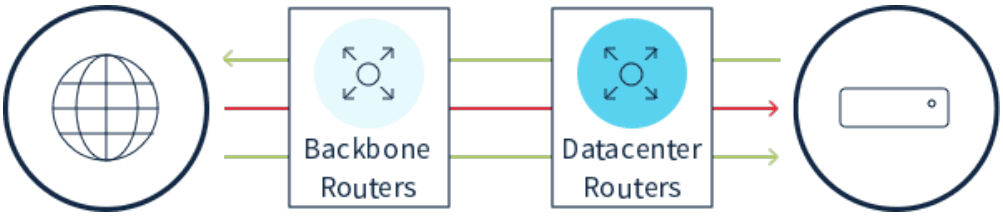
Virtual servers to manage the platform with Application Request Routing (ARR). All virtual machines have windows server datacenter operating system

Security and features

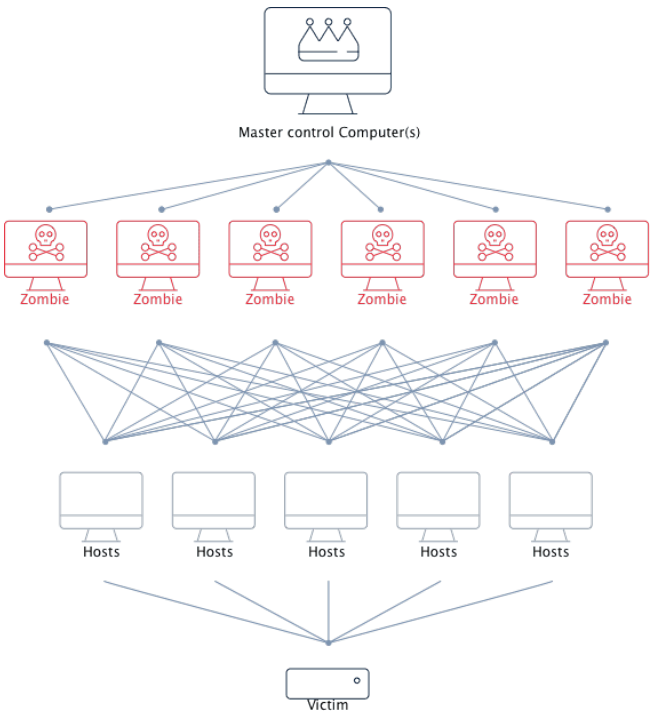
- VMware with automatic Deploy updates included
- Guaranteed bandwidth: 1.5 Gbps
- Up to 4000 pre-configured vLANs
- Support incidents 24/7/365
- Custom vSphere Client
- Resilience test
- vScope Monitoring
- Automated Host Management
- Additional dedicated resources in just 20 minutes
- Automatic Deploy
- Multi Datacenter
- 100% VMware standard
- SSL
- Backup

Anti-DDoS PRO Protection

As the volume of online data grows exponentially, Distributed Denial of Service (DDoS) attacks are becoming increasingly common.



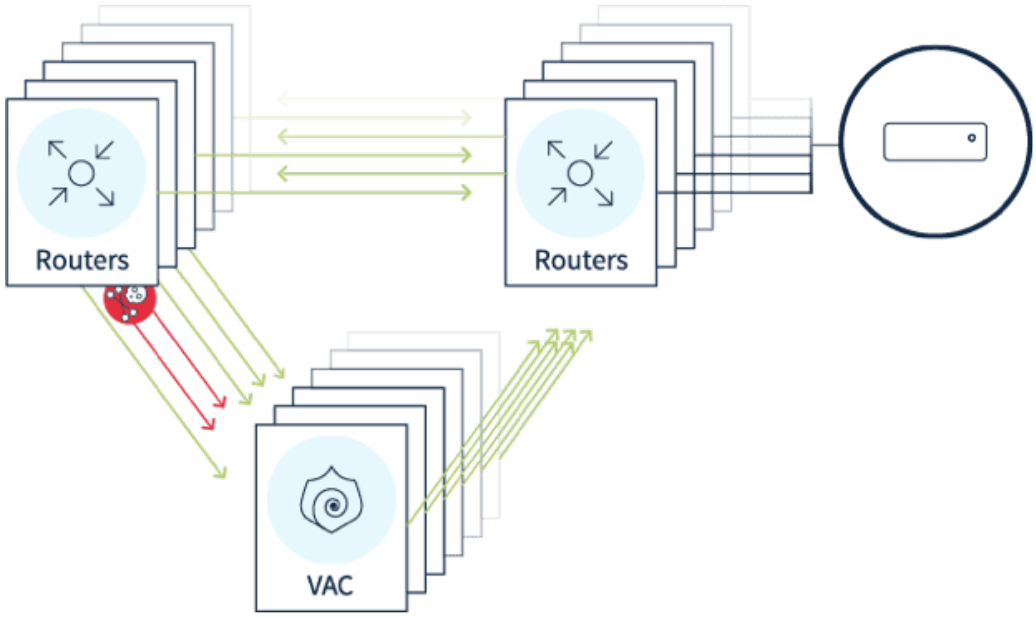
A DDoS attack aims to make a server, service or infrastructure unavailable. There are different types of attacks, such as overloading the server's bandwidth to make it unreachable, or using the machine's resources until exhausted to prevent it from responding to legitimate traffic.



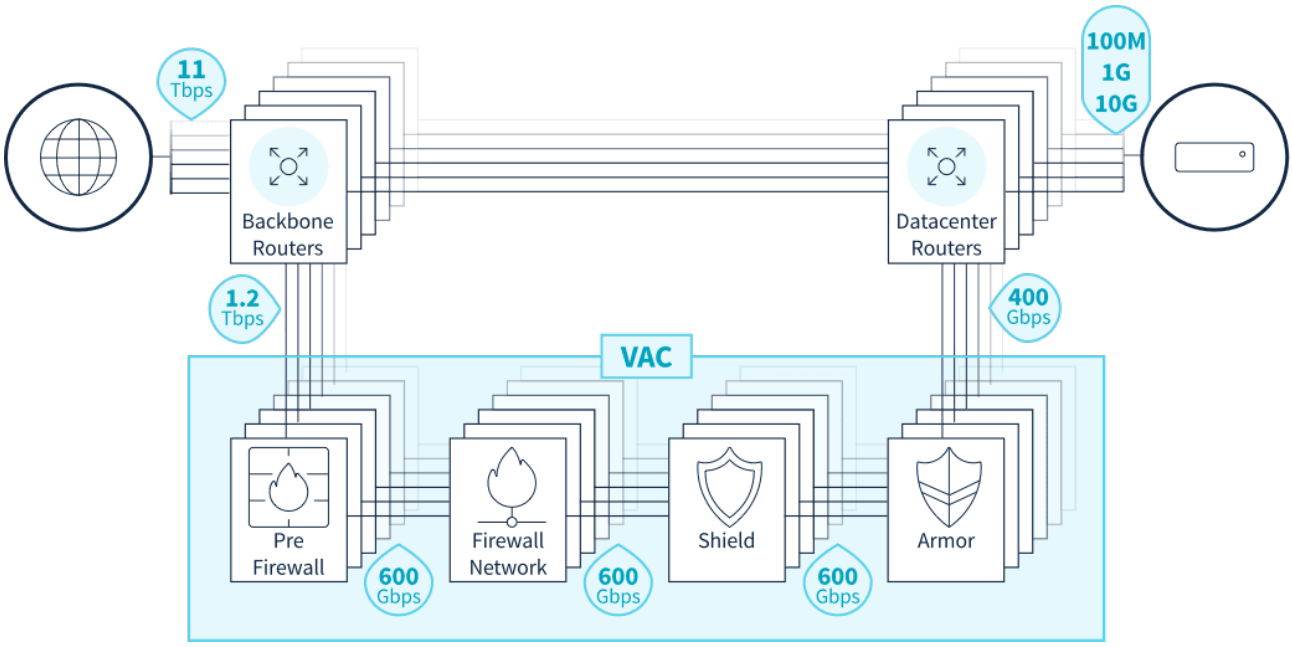
In the case of a DDoS attack, many requests are sent simultaneously from several points on the network. The intensity of this "crossfire" makes the service unstable or, worse, unavailable.

Anti-DDoS blocks this type of attack. All our services include a mitigation solution based on a unique combination of mitigation techniques:

- analyze all packages in real time and at high speed
- divert incoming traffic to your server
- Separate all non-legal IP packets from the rest, letting valid traffic pass.



VAC Components



OnCloud server farm structure certifications

The Cloud service is designed, developed and industrialized in compliance with the strictest security standards. This solution guarantees the highest level of data protection.

Transparent approach validated by a compliance process.

Our safety management systems meet the principles of ISO 27001 and comply with a number of safety standards, including: PCI DSS, HDS, TSP, CSA, ISO 27017, ISO 27018 and CISPE. Our Hosted Private Cloud infrastructures have also obtained ISO 27001, PCI DSS PSP, HDS, SOC I and II Type 2 certifications and attestations.