Data Processing Agreement pursuant to Article 28 of Regulation (EU) 2016/679 (GDPR)

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

and

IdWeb S.r.l. its registered office in via Venturelli, 11H – 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 Processor or simply PROCESSOR on the other.

WHEREAS

- a contract was subscribed between parties for the IdSurvey software, platform to design and administer CATI CAWI CAPI questionnaires;
- the Processor manages the OnCloud IdSurvey platform software as a service.

1. OBJECT OF THE AGREEMENT

This agreement has as content the regulation of the conditions that the Processor, on behalf of the CONTROLLER, commits to perform data and personal information processing operations as defined 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 PROCESSOR

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

Nature of the processing operations carried out and type of data

The processing involves the processing operations connected to the supply of IdSurvey software and the related maintenance operations.
With regard to **personal data whose transmission is implied in the use of internet communication protocol.** Those are data that are not collected to be associated with identified person, but that might, for their own nature, allow to identify users (e.g. IP address) through processing and association with data owned by third party. These data are processed for the correct website and provided service functioning and they are

acquired by IT system and software procedures during their standard functioning.
The 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 his usual activities he is, in many cases, specifically assigned to specific working phases that might involve high findings on data protection. In this cases the Processor operates as "**System Administrator"**, he 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 Processor, on behalf of the CONTROLLER, 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 controller processes in order to render the service, and by those that could be accessible to the Data 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 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 Processor during the performance of the services requested, the categories of data are those specified below by the Data Controller by ticking the box corresponding to the type of processing:

Types of data that may be accessible to the 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 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 data categories to which the Processor may accidentally access in the performance of services are processed, the Controller must indicate it by ticking the boxes indicated in the table below:

Special categories of personal data to which the 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	

In order to also highlight the presence of categories of vulnerable people, the controller declares that the data concern the following categories of interested parties:_____

_____

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 CONTROLLER

The processing Controller undertakes to:

- to provide the Processor to personal data processing in n. 2 of this agreement;
- to document in writing all instructions related to data processing by the 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 Processor;
- to supervise the processing, including the audit implementation and the inspection with the contribution of the Processor.

5. OBLIGATIONS OF THE PROCESSOR

The Processor commits in front of the Controller to:

- to treat personal data only for the **scopes** of the processing;
- to treat personal data in accordance with **instructions written** by the Controller, attached to this contract; if the Processor believes that an instruction received by the Controller 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 Controller. Moreover, if the 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 he's under, he has to inform the processing Controller 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).

6. SUB-PROCESSORS - GENERAL AUTHORIZATION

The Processor may use another Processor of processing (from now on called Sub-processor) to perform specific processing activities. In this case the processor informs in advance and in writing the Controller of all modifications related to the addition or the replacement of Sub-processors. This information have to clearly indicate the processing activities made by the Sub-processor, the identity and contact details of the Sub-processor, the date of the contract of the sub-processing. The sub-processing cannot start before the indicated term has expired without the Controller objections.

The Sub-processor has to respect duties of this contract on behalf of and according to instructions of the processing Controller. It is up to the Processor to guarantee that the Sub-processor provides the same sufficient guarantees for the implementation of technical and organizational measures adequate for the processing to satisfy requirements of the general Regulation on data processing.
If the processing Sub-processor fails to fulfill his duties on data protection, the original Processor retains the full responsibility for the fulfillment of the Sub-processor duties towards the Controller.
The sub-processors listed in Attachment C to this Agreement shall be deemed to be authorized by the Controller.

7. RIGHT OF THE DATA SUBJECTS INTERESTED TO THE REPORT

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

8. EXERCISE OF THE RIGHTS OF THE DATA SUBJECTS

The processor has to help the controller 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 processor for the exercise of their rights, the 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 controller fails to fulfill this task, the processor is free from any obligation.

9. COMMUNICATION OF A PERSONAL DATA BREACH

The Data Processor communicates to the Data Controller all personal data breach **within a maximum of 48 hours** from the moment the processor 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 Controller to legally provide, if needed, the notification of the breach to the supervisory authority.

10. ASSISTANCE FROM THE CONTROLLER TO THE DATA PROCESSOR FOR THE RESPECT OF THE DUTIES OF THE CONTROLLER, PROVIDING INFORMATION IN THEIR POSSESSION

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

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

11. SECURITY MEASURES

The processor undertakes, pursuant to Article 32, to apply security measures described in the attachment "IdSurvey OnCloud Infrastructure" that the controller declares as adequate and compliant to the instructions to provide.
The controller delegates to the Processor the adoption of different measures than those described in the attachment "IdSurvey OnCloud Infrastructure" provided that the processor respects parameters defined in the Article 32 of the Regulation. The controller and the 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 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 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 Processor also commits to directly and specifically preserve the identification details of individuals appointed as system administrators, and to promptly provide them to the Controller upon request.
Lastly, the 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 service related to the data processing, the processor is obliged to return (by downloading the data directly from the software) all personal data to the data controller, unless the latter instructs the processor to destroy them.
The return is accompanied by the destruction of all copies existing in the computer system of the processor.

13. DATA PROTECTION OFFICER (DPO OR RPD)

The Data Processor is not obliged to nominate a Data protection officer (DPO or RPD). He commits anyway to publish the contact details of the data protection officer, if one is nominated.

14. RECORDS OF PROCESSING ACTIVITIES

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

15. DOCUMENTATION

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

16. FINAL CLAUSES

The recitals and annexes form an integral part of this agreement.
By signing this agreement, the Controller, without prejudice to the provisions of Regulation (EU) 2016/679 and in compliance with the principles of accountability and control, acknowledges that, in accordance with this agreement and in particular with the provisions of Section 5, and limited to the service covered by this agreement, should the Processor engage a sub-processor that transfers data to third countries, it may propose the adoption of the Standard Contractual Clauses set out in Commission Implementing Decision (EU) 2021/914 of 4 June 2021, exclusively with reference to the relevant modules, namely from processor to processor (P2P) and from processor to controller (P2C), as well as any supplementary contractual measures accompanying them. The effectiveness of such Clauses in relation to the modules from controller to controller (C2C) and from controller to processor (C2P), and of the related supplementary measures, is expressly subject to the prior written approval of the Controller.

This agreement constitutes implementation of the reference made in the "confidentiality and privacy" clauses contained in the IdSurvey contract and entirely supersedes and replaces any act or agreement, whether written or oral, previously entered into between the parties governing the same subject matter.

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 Controller

_____

The Processor

_____

Pursuant to and for the effects of Articles 1341 and 1342 the Controller declares to expressly approve clauses n. 16 (Mandate to sign standard clauses and additional contractual measures) 17 (competent court) and 18 (applicable law)

Place _____ Date _____

The Controller

_____

Attachment A

Controller's DPO name (if applicable)	Contact Information

Attachment B - Contact details

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

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

Contact details of the 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 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 Processor.

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

Sub-processor	Contact details	DPO	Used for
AD CONSULTING S.p.A	Via Pier Paolo Pasolini n.15 41123 Modena (MO) P. IVA/C.F. 03410070365	dpo@adcgroup.com	Azure Cloud
The Rocket Science Group , LLC	Sede Legale: 675 Ponce de Leon Ave. NE, Atlanta, Georgia 30308, US .	dpo@mailchimp.com	Email-Sender
ONLINECITY.IO ApS VAT. no. DK27364276	Buchwaldsgade 50 - 5000 Odense C - Danmark Tel (+45) 6611 8311 e-mail tinfo@onlinecity.io	N.A.	SMS-Sender
OpenAI OpCo, LLC	1455 3rd Street, San Francisco, CA 94158	privacy@openai.com	Codifica risposte AI Analisi e report Insight AI

Personal data outside the EU are transferred only in the event that the Controller uses the email delivery system integrated in IdSurvey (EmailSender), and such transfer is strictly limited to the email address and the content of the email itself.

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

The table of sub-processors will be updated from time to time and the Controller 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 person in charge to the Controller (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 Controller's systems); • alteration (the data is present on the systems but has been altered); • deletion (the data are no longer on the Controller's systems and neither has the author of the violation); • theft (the data are no longer on the Controller'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 Controller's systems); • alteration (the data is present on the systems but has been altered); • deletion (the data are no longer on the Controller's systems and neither has the author of the violation); • theft (the data are no longer on the Controller'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 Controller or the 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 Controller to the Data Processor

The 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 Processor and the Data Controller and, where applicable, the Data Protection Officer;
    - the categories of processing carried out on behalf of the Data Controller;
    - 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 Attachment "IdSurvey infrastructure on Cloud";
- **notify the Data Controller 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 Controller in order to jointly agree on the response. T The Data Controller will also be promptly notified of any information transmitted by sub-controllers regarding government access requests from authorities and 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 owner through the idsurvey control panel, in relation to data downloading (portability), deletion, copying, generation of authentication profiles and permissions, etc., which shall be considered "written instructions" under this Agreement.

ATTACHMENT F
Information about processing carried out abroad

Service	Sub-processor	Third country to which data is transferred	Safeguard measure
Mailchimp (EmailSender)	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 Controller and Data Processor, the Data Controller shall be deemed to have been informed of the transfers made in third countries as described in this Attachment**.

Personal data outside the EU are transferred only in the event that the Controller makes use of the email delivery system integrated in IdSurvey (EmailSender), and such transfer is strictly limited to the email address and the content of the email itself.

ANNEX 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 level of security, we employ effective devices and adopt a series of best practices at all levels of our organization and infrastructure.

Datacenter Security

- Data centers compliant with industry standards, such as ISO/IEC 27001:2013 and NIST SP 800-53, ensuring security and reliability.
- Physical access to servers restricted to accredited personnel only.
- Access to data centers allowed exclusively through multi-factor authentication systems for accredited personnel.
- 24/7 video and human surveillance.
- Facilities equipped with smoke particle detection and fire suppression systems.
- Technical staff available 24 hours a day, 7 days a week.
- Data centers equipped with redundant power systems, including UPS and generators, to ensure service continuity in the event of power outages.
- Microsoft Azure complies with a wide range of international standards (ISO/IEC 27018, SOC 1/2/3, GDPR, CSA STAR, etc.), ensuring compliance with data protection regulations.

Security and Features

- Microsoft Azure infrastructure based on Hyper-V technology and native cloud services, with automatic updates and security patches included.
- High-performance connectivity through Microsoft's global network, with broad bandwidth availability.
- Support for isolated virtual networks (Azure Virtual Network) with secure and scalable subnet management.
- Microsoft support for incidents 24/7/365.
- Azure portal and APIs for cloud resource management.
- Integrated tools for resilience testing and business continuity verification.
- Advanced monitoring services via Azure Monitor and Application Insights.
- Automated host infrastructure management with transparent updates and maintenance.
- On-demand scalability of resources with rapid provisioning.
- Automatic deployment.
- Local Redundancy Storage.
- System based on internationally recognized Microsoft Azure standards.
- SSL.
- Backup through Azure Backup and redundant solutions.
- Firewall and network: Azure Firewall, Network Security Groups, and network-level protections.

Anti-DDoS PRO Protection

With the exponential growth of online data volumes, Distributed Denial of Service (DDoS) attacks are becoming increasingly frequent.

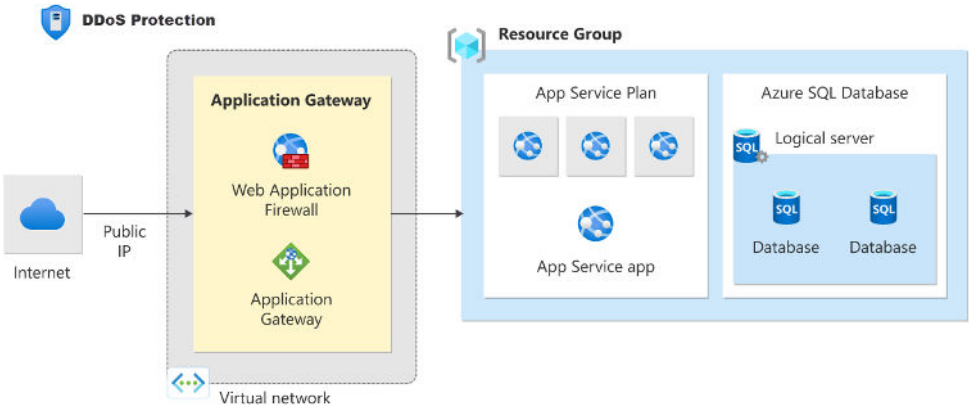
A DDoS attack aims to render servers, applications, or entire infrastructures unavailable by overloading bandwidth or exhausting computing resources until their response capacity is blocked.

To ensure service continuity, Microsoft Azure integrates DDoS Protection.

This protection is based on automatic mitigation techniques that allow for:

- real-time, high-speed analysis of network traffic,
- identification and diversion of malicious traffic before it reaches resources,
- filtering of illegitimate packets and allowing only valid traffic.

This protection is active 24/7 and leverages Microsoft's global network to ensure resilience even against large-scale attacks.



Server Farm OnCloud Infrastructure Certifications

The Cloud service is designed and developed in accordance with the most rigorous international security standards, following a Security by Design and Defense in Depth approach, ensuring the highest level of data protection.

Microsoft Azure adopts a transparent approach and undergoes regular independent audit processes. Its security management systems are certified under ISO/IEC 27001 and compliant with numerous other standards, including:

- ISO/IEC 27017 (security controls specific to the cloud),
- ISO/IEC 27018 (protection of personal data in the cloud),
- SOC 1, SOC 2, and SOC 3,
- PCI DSS (payment data security),
- CSA STAR (Cloud Security Alliance Security, Trust & Assurance Registry),
- GDPR compliance for personal data protection,
- FedRAMP and HIPAA for specific international regulatory requirements.

The updated and complete list of certifications is available here: https://learn.microsoft.com/en-us/azure/compliance/