Data Protection Policy

Last updated	December 01, 2021
Applies to	This will apply to all services within Omni Sp. z o. o. (LLC)
To be reviewed	Every three years

Definitions

Company	Omni Sp. z o. o. (LLC), a registered under the laws of Poland with the office at at Hoża str., bld 86, room 210, Warszawa 00-682, Poland.
GDPR	means the General Data Protection Regulation.
Responsible Person	means Company's Director responsible for data protection within the Company.
Register of Systems	means a register of all systems or contexts in which personal data is processed by the Company.

1 INTRODUCTION

The Company is committed to conducting its business in accordance with all applicable Data Protection laws and regulations and in line with the highest standards of ethical conduct. This policy sets forth the expected behaviors of Company's Employees and Third Parties in relation to the collection, use, retention, transfer, disclosure and destruction of any Personal Data belonging to a Company Contact (i.e., the Data Subject).

Personal Data is any information (including opinions and intentions, content of messages and etc.) which relates to an identified or identifiable Natural Person. Personal Data is subject to certain legal safeguards and other regulations, which impose restrictions on how legal entities may process Personal Data. The Company is responsible for ensuring compliance with the Data Protection requirements outlined in this policy. Non-compliance may expose Company to complaints, regulatory action, fines and/or reputational damage. The Company's leadership is fully committed to ensuring continued and effective implementation of this policy, and expects all Company's Employees and Third Parties to share in this commitment. Any breach of this policy will be taken seriously and may result in disciplinary action or business sanction.

2 LEGAL FRAMEWORK

The General Data Protection Regulation (EU) 2016/679 (GDPR) Data Protection Act 1988

3 SCOPE

This policy applies to all Company's Employees and all third parties responsible for the processing of personal data on behalf of Company's services.

4 POLICY

4.1 Responsible person

To demonstrate our commitment to GDPR, and to enhance the effectiveness of our compliance efforts, Company has the Responsible person. The Responsible person's duties include:

a) informing and advising Company and its Employees who carry out Processing pursuant to Data Protection regulations, national law or Union based Data Protection provisions;

b) ensuring the alignment of this policy with Data Protection regulations, national law or Union based Data Protection provisions;

c) providing guidance with regards to carrying out Data Protection Impact Assessments (DPIAs);

d) acting as a point of contact for and cooperating with Data Protection Authorities (DPAs);

e) determining the need for notifications to one or more DPAs as a result of Company's current or intended Personal Data processing activities;

f) making and keeping current notifications to one or more DPAs as a result of Company's current or intended Personal Data processing activities;

g) the establishment and operation of a system providing prompt and appropriate responses to Data Subject requests;

h) informing shareholders and owners of Company of any potential corporate, civil and criminal penalties which may be levied against Company and/or its Employees for violation of applicable Data Protection laws. Ensuring establishment of procedures and standard contractual provisions for obtaining compliance with this Policy by any Third Party who:

- provides Personal Data to the Company's Service,
- receives Personal Data from the Company's Service,
- has access to Personal Data collected or processed by Company's Service.

4.2 Data Protection by Design

To ensure that all Data Protection requirements are identified and addressed when designing new systems or processes and/or when reviewing or expanding existing sys-

tems or processes, each of them must go through an approval process before continuing. Each Company's Service must ensure that a Data Protection Impact Assessment (DPIA) is conducted, in cooperation with the Responsible person, for all new and/or revised systems or processes for which it has responsibility. Where applicable, the Information Technology (IT) department, as part of its IT system and application design review process, will cooperate with the Responsible person of Data Protection to assess the impact of any new technology uses on the security of Personal Data.

4.3 Compliance Monitoring

To confirm that an adequate level of compliance that is being achieved by all Company's Services in relation to this policy, the Responsible person will carry out an annual Data Protection compliance audit for all such Services. Each audit will, as a minimum, assess:

a) Compliance with Policy in relation to the protection of Personal Data, including: the assignment of responsibilities, raising awareness, training of Employees.

b) The effectiveness of Data Protection related operational practices, including: Data Subject rights; Personal Data transfers; Personal Data incident management; Personal Data complaints handling.

c) The level of understanding of Data Protection policies and Privacy Notices.

d) The currency of Data Protection policies and Privacy Notices.

e) The accuracy of Personal Data being stored.

f) The conformity of Data Processor activities.

g) The adequacy of procedures for redressing poor compliance and Personal Data Breaches. The Responsible person, in cooperation with key business stakeholders from each Company's Service, will devise a plan with a schedule for correcting any identified deficiencies within a defined and reasonable time frame. Any major deficiencies and good practice identified will be reported to, monitored and shared by the Responsible person.

5 DATA PROTECTION PRINCIPLES

The Company is committed to processing data in accordance with its responsibilities under the GDPR.

Article 5 of the GDPR requires that personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals.

This means, Company must tell the Data Subject what Processing will occur (transparency), the Processing must match the description given to the Data Subject (fairness), and it must be for one of the purposes specified in the applicable Data Protection regulation (lawfulness);

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) company must not store any Personal Data beyond what is strictly required;

d) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

   This means Company must specify exactly what the Personal Data collected will be used for and limit the Processing of that Personal Data to only what is necessary to meet the specified purpose.

e) Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

   This means Company must have in place processes for identifying and addressing out-of-date, incorrect and redundant Personal Data;

f) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organizational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

g) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.

6 DATA COLLECTION

6.1 Data Sources

Personal Data should be collected only from the Data Subject unless one of the following apply:

a) The nature of the business purpose necessitates collection of the Personal Data from other persons or bodies.

b) The collection must be carried out under emergency circumstances in order to protect the vital interests of the Data Subject or to prevent serious loss or injury to another person.

c) If Personal Data is collected from someone other than the Data Subject, the Data Subject must be informed of the collection unless one of the following apply:

d) The Data Subject has received the required information by other means.

e) The information must remain confidential due to a professional secrecy obligation

f) A national law expressly provides for the collection, Processing or transfer of the Personal Data.

g) Where it has been determined that notification to a Data Subject is required, notification should occur promptly, but in no case later than:

- One calendar month from the first collection or recording of the Personal Data
- At the time of first communication if used for communication with the Data Subject
- At the time of disclosure if disclosed to another recipient.

6.2 Data Subject Consent

Each Company's Service will obtain Personal Data only by lawful and fair means and, where appropriate with the knowledge and Consent of the individual concerned. Where a need exists to request and receive the Consent of an individual prior to the collection, use or disclosure of their Personal Data, Company is committed to seeking such Consent. The Responsible person, in cooperation with other relevant business representatives, shall establish a system for obtaining and documenting Data Subject Consent for the collection, Processing, and/or transfer of their Personal Data.

6.3 Data Subject Notification

Each Company's Service will, when required by applicable law, contract, or where it considers that it is reasonably appropriate to do so, provide Data Subjects with information as to the purpose of the Processing of their Personal Data. When the Data Subject is asked to give Consent to the Processing of Personal Data and when any Personal Data is collected from the Data Subject, all appropriate disclosures will be made, in a manner that draws attention to them, unless one of the following apply:

a) The Data Subject already has the information

b) A legal exemption applies to the requirements for disclosure and/or Consent.

The disclosures may be given orally, electronically or in writing. If given orally, the person making the disclosures should use a suitable script or form approved in advance by the Company. The associated receipt or form should be retained, along with a record of the facts, date, content, and method of disclosure.

6.4 External Privacy Notices

Each external website provided by Company will include an online 'Privacy Notice' and an online 'Cookie Notice' fulfilling the requirements of applicable law.

6.5 Data Use

Data Processing Company uses the Personal Data of its Contacts for the following broad purposes:

a) The general running and business administration of Company's Services.

b) To provide information to Company Shareholder.

c) The ongoing administration and management of customers services.

The use of a Contact's information should always be considered from their perspective and whether the use will be within their expectations or if they are likely to object. Each Company's service will Process Personal Data in accordance with all applicable laws and applicable contractual obligations.

More specifically, Company will not Process Personal Data unless at least one of the following requirements are met:

a) The Data Subject has given Consent to the Processing of their Personal Data for one or more specific purposes.

b) Processing is necessary for the performance of a contract to which the Data Subject is party or in order to take steps at the request of the Data Subject prior to entering into a contract.

c) Processing is necessary for compliance with a legal obligation to which the Data Controller is subject.

d) Processing is necessary in order to protect the vital interests of the Data Subject or of another natural person.

e) Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Data Controller.

f) Processing is necessary for the purposes of the legitimate interests pursued by the Data Controller or by a Third Party (except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject, in particular where the Data Subject is a child).

There are some circumstances in which Personal Data may be further processed for purposes that go beyond the original purpose for which the Personal Data was collected. When making a determination as to the compatibility of the new reason for Processing, guidance and approval must be obtained from the Responsible person before any such Processing may commence.

a) In any circumstance where Consent has not been gained for the specific Processing in question, Company will address the following additional conditions to determine the fairness and transparency of any Processing beyond the original purpose for which the Personal Data was collected: Any link between the purpose

for which the Personal Data was collected and the reasons for intended further Processing.

b) The context in which the Personal Data has been collected, in particular regarding the relationship between Data Subject and the Data Controller.

c) The nature of the Personal Data, in particular whether Special Categories of Data are being Processed, or whether Personal Data related to criminal convictions and offences are being Processed.

d) The possible consequences of the intended further Processing for the Data Subject.

e) The existence of appropriate safeguards pertaining to further Processing, which may include Encryption, Anonymization or Pseudonymization.

To ensure its processing of data is lawful, fair and transparent, the Company shall maintain a Register of operations. The Register of operations shall be reviewed at least annually. Individuals have the right to access their personal data and any such requests made to the Company shall be dealt with in a timely manner.

All data processed by the Company must be done on one of the following lawful bases: consent, contract, legal obligation, vital interests, public task or legitimate interests. The Company shall note the appropriate lawful basis in the Register of operations.

6.6 Special Categories of Data

Company will only Process Special Categories of Data (also known as sensitive data) where the Data Subject expressly consents to such Processing or where one of the following conditions apply:

a) The Processing relates to Personal Data which has already been made public by the Data Subject.

b) The Processing is necessary for the establishment, exercise or defense of legal claims.

c) The Processing is specifically authorized or required by law.

d) The Processing is necessary to protect the vital interests of the Data Subject or of another natural person where the Data Subject is physically or legally incapable of giving consent.

e) Further conditions, including limitations, based upon national law related to the Processing of genetic data, biometric data or data concerning health.

In any situation where Special Categories of Data are to be Processed, prior approval must be obtained from the Responsible person, and the basis for the Processing clearly recorded with the Personal Data in question. Where Special Categories of Data are being Processed, Company will adopt additional protection measures.

6.7 Children's Data

The Company doesn't have the intention for processing and/or transfer of data from and to children under 18 years of age. Children under 18 years are recommended not to provide us with any personal information. If the Company finds that a person under age of 18 has provided us with such information through the web-site, we will use reasonable efforts to remove that information from our databases.

Meanwhile children under the age of 18 are unable to Consent to the Processing of Personal Data for information society services (any service normally provided for payment, by electronic means and at the individual request of a recipient of services). Consent must be sought from the person who holds parental responsibility over the child. However, it should be noted that where Processing is lawful under other grounds, Consent need not be obtained from the child or the holder of parental responsibility.

6.8 Data Quality

Each Company's Service will adopt all necessary measures to ensure that the Personal Data it collects and Processes is complete and accurate in the first instance, and is updated to reflect the current situation of the Data Subject. The measures adopted by Company to ensure data quality include:

a) Correcting Personal Data known to be incorrect, inaccurate, incomplete, ambiguous, misleading or outdated, even if the Data Subject does not request rectification.

b) Keeping Personal Data only for the period necessary to satisfy the permitted uses or applicable statutory retention period.

c) The removal of Personal Data if in violation of any of the Data Protection principles or if the Personal Data is no longer required.

d) Restriction, rather than deletion of Personal Data, insofar as:

- a law prohibits erasure.
- erasure would impair legitimate interests of the Data Subject.
- the Data Subject disputes that their Personal Data is correct and it cannot be clearly ascertained whether their information is correct or incorrect.

6.9 Profiling & Automated Decision-Making

Company will only engage in Profiling and automated decision-making where it is necessary to enter into, or to perform, a contract with the Data Subject or customer or where it is authorized by law. Where a Company Service/Entity utilizes Profiling and automated decision-making, this will be disclosed to the relevant Data Subjects. In such cases the Data Subject will be given the opportunity to:

- Express their point of view.

- Obtain an explanation for the automated decision.
- Review the logic used by the automated system.
- Supplement the automated system with additional data.
- Have a human carry out a review of the automated decision.
- Contest the automated decision. Object to the automated decision-making being carried out.

Each Company's Service must also ensure that all Profiling and automated decision-making relating to a Data Subject is based on accurate data.

6.10 Digital Marketing

As a rule, Company will not send promotional or direct marketing material to Company's Contact through digital channels such as mobile phones, messengers, email and the Internet, without first obtaining their Consent (directly or through the Company's customers who are the Data Controllers).

Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the personal data. Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent should be clearly available and systems should be in place to ensure such revocation is reflected accurately in the Company's systems.

Any Company's Service wishing to carry out a digital marketing campaign without obtaining prior Consent from the Data Subject must first have it approved by the Responsible person. Where Personal Data Processing is approved for digital marketing purposes, the Data Subject must be informed at the point of first contact that they have the right to object, at any stage, to having their data Processed for such purposes. If the Data Subject puts forward an objection, digital marketing related Processing of their Personal Data must cease immediately and their details should be kept on a suppression list with a record of their opt-out decision, rather than being completely deleted. It should be noted that where digital marketing is carried out in a 'business to business' context, there is no legal requirement to obtain an indication of Consent to carry out digital marketing to individuals provided that they are given the opportunity to opt-out.

6.11 Data Retention

To ensure fair Processing, Personal Data will not be retained by Company for longer than necessary in relation to the purposes for which it was originally collected, or for which it was further Processed. The length of time for which Company services need to retain Personal Data is set out in Company's archiving policy. This takes into account the legal and contractual requirements, both minimum and maximum, that influence the retention periods set forth in the schedule. All Personal Data should be deleted or

destroyed after 5 (five) years since the last Data Subject inactivity[1] or until the consent is revoke/you have objected to such processing.

The archiving policy shall be reviewed annually.

The Company shall ensure that personal data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

The Company shall take reasonable steps to ensure personal data is accurate.

Where necessary for the lawful basis on which data is processed, steps shall be put in place to ensure that personal data is kept up to date.

The Company shall ensure that personal data is stored securely using modern software that is kept-up-to-date.

Access to personal data shall be limited to personnel who need access and appropriate security should be in place to avoid unauthorized sharing of information. When personal data is deleted, this should be done safely such that the data is irrecoverable. Appropriate back-up and disaster recovery solutions shall be in place.

6.12 Data Protection

Each Company's Service will adopt physical, technical, and organizational measures to ensure the security of Personal Data. This includes the prevention of loss or damage, unauthorized alteration, access or Processing, and other risks to which it may be exposed by virtue of human action or the physical or natural environment. A summary of the Personal Data related security measures is provided below:

a) Prevent unauthorized persons from gaining access to data processing systems in which Personal Data are Processed.

b) Prevent persons entitled to use a data processing system from accessing Personal Data beyond their needs and authorizations.

c) Ensure that Personal Data in the course of electronic transmission during transport cannot be read, copied, modified or removed without authorization.

d) Ensure that access logs are in place to establish whether, and by whom, the Personal Data was entered into, modified on or removed from a data processing system.

e) Ensure that in the case where Processing is carried out by a Data Processor, the data can be Processed only in accordance with the instructions of the Data Controller.

[1] Inactive means Data Subject has not interacted (opened, clicked, replied emails, answered phone calls, responded to text messages that we have sent them) since the last activity. From time to time, it may be necessary to retain or access historic personal data under certain circumstances such as if we have contractually agreed to do so or if we have become involved in unforeseen events like litigation or business disaster recoveries.

f) Ensure that Personal Data is protected against undesired destruction or loss.

g) Ensure that Personal Data collected for different purposes can and is Processed separately.

h) Ensure that Personal Data is not kept longer than necessary

6.13 Data Subject Requests

The Responsible person will establish a system to enable and facilitate the exercise of Data Subject rights related to:

- Information access.
- Objection to Processing.
- Objection to automated decision-making and profiling.
- Restriction of Processing.
- Data portability.
- Data rectification.
- Data erasure.

If an individual makes a request relating to any of the rights listed above Company will consider each such request in accordance with all applicable Data Protection laws and regulations. No administration fee will be charged for considering and/or complying with such a request unless the request is deemed to be unnecessary or excessive in nature.

Data Subjects are entitled to obtain, based upon a request made in writing/email to Responsible person: Chairman of the Board OMNI SP. Z O. O. (LLC) Jarosław Wiczyński, address: Skr. poczt. 268 str. Jagiellońska 6 85-001 Bydgoszcz Poland, e-mail: info@omniomni.io.

It should be noted that situations may arise where providing the information requested by a Data Subject would disclose Personal Data about another individual. In such cases, information must be redacted or withheld as may be necessary or appropriate to protect that person's rights.

6.14 Law Enforcement Requests & Disclosures

In certain circumstances, it is permitted that Personal Data be shared without the knowledge or Consent of a Data Subject. This is the case where the disclosure of the Personal Data is necessary for any of the following purposes:

- the prevention or detection of crime;
- the apprehension or prosecution of offenders;
- the assessment or collection of a tax or duty;

- by the order of a court or by any rule of law.

If a Company service Processes Personal Data for one of these purposes, then it may apply an exception to the Processing rules outlined in this policy but only to the extent that not doing so would be likely to prejudice the case in question. If any Company Service receives a request from a court or any regulatory or law enforcement authority for information relating to a Company Contact, you must immediately notify the Responsible person who will provide comprehensive guidance and assistance.

6.15 Data Protection Training

All Company's Employees that have access to Personal Data will have their responsibilities under this policy outlined to them as part of their staff induction training.

6.16 Data Transfers

Company Services may transfer Personal Data to internal or Third-Party recipients located in another country where that country is recognized as having an adequate level of legal protection for the rights and freedoms of the relevant Data Subjects. Where transfers need to be made to countries lacking an adequate level of legal protection (i.e., Third Countries), they must be made in compliance with an approved transfer mechanism. Company Services may only transfer Personal Data where one of the transfer scenarios lists below applies:

- The Data Subject has given Consent to the proposed transfer.
- The transfer is necessary for the performance of a contract with the Data Subject
- The transfer is necessary for the implementation of pre-contractual measures taken in response to the Data Subject's request.
- The transfer is necessary for the conclusion or performance of a contract concluded with a Third Party in the interest of the Data Subject.
- The transfer is legally required on important public interest grounds.
- The transfer is necessary for the establishment, exercise or defense of legal claims.
- The transfer is necessary in order to protect the vital interests of the Data Subject.

6.16.1 Transfers to Third Parties

Each Company Service will only transfer Personal Data to, or allow access by, Third Parties when it is assured that the information will be Processed legitimately and protected appropriately by the recipient. Where Third Party Processing takes place, each Company Service/Entity will first identify if, under applicable law, the Third Party is considered a Data Controller or a Data Processor of the Personal Data being transferred. Where the Third Party is deemed to be a Data Controller, Company Service will enter into, in cooperation with the Responsible person, an appropriate agreement with the

Controller to clarify each party's responsibilities in respect to the Personal Data transferred. Where the Third Party is deemed to be a Data Processor, Company Service will enter into, in cooperation with the Responsible person, an adequate Processing agreement with the Data Processor. The agreement must require the Data Processor to protect the Personal Data from further disclosure and to only Process Personal Data in compliance with Company instructions. In addition, the agreement will require the Data Processor to implement appropriate technical and organizational measures to protect the Personal Data as well as procedures for providing notification of Personal Data Breaches. Company has a 'Standard Data Processing Agreement' document that, should be used as a baseline template. When a Company Service is outsourcing services to a Third Party (including Cloud Computing services), they will identify whether the Third Party will Process Personal Data on its behalf and whether the outsourcing will entail any Third Country transfers of Personal Data. In either case, it will make sure to include, in cooperation with the Responsible person, adequate provisions in the outsourcing agreement for such Processing and Third Country transfers. The Responsible person shall conduct regular audits of Processing of Personal Data performed by Third Parties, especially in respect of technical and organizational measures they have in place.

6.17 Complaints Handling

Data Subjects with a complaint about the Processing of their Personal Data, should put forward the matter in writing to the Responsible person. An investigation of the complaint will be carried out to the extent that is appropriate based on the merits of the specific case. The Responsible person will inform the Data Subject of the progress and the outcome of the complaint within a reasonable period. If the issue cannot be resolved through consultation between the Data Subject and the Responsible person, then the Data Subject may, at their option, seek redress through mediation, binding arbitration, litigation, or via complaint to the Data Protection Authority within the applicable jurisdiction.

6.18 Breach

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data, the Company shall promptly assess the risk to people's rights and freedoms and if appropriate report this breach to the Data Protection Authority.

Any individual who suspects that a Personal Data Breach has occurred due to the theft or exposure of Personal Data must immediately notify the Responsible person providing a description of what occurred. Notification of the incident can be made via e-mail: info@omniomni.io. The Responsible person will investigate all reported incidents to confirm whether or not a Personal Data Breach has occurred. If a Personal Data Breach

is confirmed, the Responsible person will follow the relevant authorized procedure based on the criticality and quantity of the Personal Data involved.

7 ROLES & RESPONSIBILITIES

7.1 Implementation

The management team of the Company must ensure that all Company's Employees responsible for the Processing of Personal Data are aware of and comply with the contents of this policy. In addition, each Company Service will make sure all Third Parties engaged to Process Personal Data on their behalf (i.e., their Data Processors) are aware of and comply with the contents of this policy. Assurance of such compliance must be obtained from all Third Parties, whether companies or individuals, prior to granting them access to Personal Data controlled by the Company.

7.2 Support, Advice and Communication

For advice and support in relation to this policy, please contact the Responsible person on email info@omniomni.io.

7.3 Review

This policy will be reviewed by the Responsible person every three years, unless there are any changes to regulations or legislation that would enable a review earlier.

END OF POLICY