PRIVACY POLICY

Pappu Hybrid Pallet Limited Company (hereinafter: Data Controller) considers it extremely important to respect the right of his partners, customers and visitors to informational self-determination. The Data Controller handles personal data confidentially, in accordance with the applicable European Union and domestic legislation and the relevant data protection (authority) practice and takes all security and organizational measures that guarantee the security, confidentiality, integrity and availability of the data.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter referred to as GDPR) and, taking into account the provisions of Irish legislation in force, the following notice for the protection of personal data processed(hereinafter referred to as: Policy).

The Policy is effective from 01 December 2024 to the date of withdrawal in relation to the processing of personal data of data subjects in the activities carried out by the Data Controller.

The Data Controller reserves the right to unilaterally change this Policy at any time. If the Policy is amended, the Data Controller shall inform the data subjects thereof.

THE CONTROLLER

Name of data controller:	Pappu Hybrid Pallet Limited Company
E-mail address:	pappu@papputhehybridpallet.com

DATA PROCESSING IN CONNECTION WITH THE PERFORMANCE OF A CONTRACT

The Data Controller processes personal data as a result of its activities presented on its website. The Data Controller shall endeavour to process only the personal data necessary for the performance of the contract. The Data Controller processes the personal data obtained during the performance of the contract as follows:

Scope of personal data processed: The Data Controller processes the natural person contracted with it and the sole proprietor for the purpose of performing the contract

- first and last name,
- Titulusate,
- birth surname and first name,
- place and date of birth,
- mother's name,
- address,
- identity card number,
- address or address of registered office, establishment,
- the address of the property covered by the contract,
- Phone number
- your e-mail address,
- bank account number,
- other data and information (e.g. interests, information about borrowing, financial information).

For the purpose of fulfilling the contract and maintaining contact, the Data Controller manages it as the contact person of the legal entity contracted with it

- first and last name,
- titulusate,

- place of work,
- position, job title,
- address or address of registered office, establishment,
- the address of the property covered by the contract,
- Phone number
- your e-mail address,
- other data and information (e.g. interests, information about borrowing, financial information).

Categories of data subjects: data subjects intending to establish a business relationship with the Data Controller or already in a contractual relationship.

Source of processed personal data: the data subject.

Purpose of data processing: performance of contract.

Legal basis for data processing: performance of a contract between the Data Controller and the data subject pursuant to Article 6 (1) (b) of the GDPR within the scope of the agreement, conclusion of a contract.
In the course of legal or enforcement of claims and in the processing of contact data of legal persons, pursuant to Article 6 (1) (f) of the GDPR, the legitimate interest of the Data Controller.

Duration of data processing: 5 years after the existence of the contractual or business relationship or the capacity of the data subject's representative (general limitation period for enforcement). Upon expiry of the general limitation period for enforcement or a longer retention period specified by law, personal data, including contact details, will be deleted immediately and irretrievably.

Access: the Data Controller has primary access to the personal data processed in connection with the performance of the contract with the Data Controller.

Data transfer: personal data will not be transferred to third parties, unless otherwise provided for in the contract between the data subject and the Data Controller.

Technique of data processing: the Data Controller processes the personal data of the data subject electronically.

Profiling: the Data Controller does not make decisions based solely on automated data processing in relation to the data subject, nor does it create a profile about the data subject based on the available personal data.

Rights of data subjects: in connection with data processing, data subjects may exercise the rights of access, rectification, erasure, restriction of processing, data portability and objection.

DATA PROCESSING IN CONNECTION WITH CONTACT

Direct and fast contact and communication between the Data Controller and the data subject is essential for the management of the contractual partner in partnership with the Data Controller, for the organization of work and for ensuring appropriate working conditions. For the purpose of contact, the Data Controller processes personal data as follows:

Scope of personal data processed: title, first and last name, phone number, e-mail address.

Categories of data subjects: data subjects intending to enter into a cooperation relationship with the Data Controller or already in a contractual relationship, as well as contact persons of legal entities.

Source of processed personal data: the data subject.

Purpose of data processing: communication between the Data Controller and the data subject.

Legal basis for data processing: pursuant to Article 6 (1) (f) of the GDPR, the legitimate economic interest of the Data Controller in connection with contact.

Duration of data processing: 5 years after the existence of the contractual or business relationship or the capacity of the data subject's representative (general limitation period for enforcement). Upon expiry of the general limitation period for enforcement or a longer retention period specified by law, personal data, including contact details, will be deleted immediately and irretrievably.

Access: the personal data processed for contact purposes may primarily be accessed by the Data Controller. If proceedings are initiated before a court or other authority which require the transfer of personal data to the court or authority, the court or authority may also have access to the personal data.

Data transfer: personal data will not be transferred to third parties, unless otherwise provided for in the contract between the data subject and the Data Controller.

Technique of data processing: the Data Controller processes the personal data of the data subject electronically in its electronic records.

Profiling: the Data Controller does not make decisions based solely on automated data processing in relation to the data subject, nor does it create a profile about the data subject based on the available personal data.

Rights of data subjects: in connection with data processing, data subjects may exercise the rights of access, rectification, erasure, restriction of processing and objection.

DATA PROCESSING IN CONNECTION WITH COMPLAINT HANDLING

The Data Controller accepts complaints received in writing (on its website, by post or email) in connection with the performance of its activities and the provision of services presented on its website. Within this framework, the Data Controller processes the personal data of the data subject as follows:

Scope of personal data processed: first and last name, title, contact data (e-mail address, telephone number), address, other personal data provided by the complainant in connection with the complaint, case number, signature, in case of the assistance of an authorized agent, the first and last name, title, place and date of birth, mother's name.

Categories of data subjects: data subjects submitting complaints to the Data Controller.

Source of processed personal data: the data subject.

Purpose of data processing: investigation and remedy of complaints.

Legal basis for data processing: pursuant to Article 6 (1) (f) of the GDPR, the legitimate interest of the Data Controller.

Duration of data processing: redress of complaint, maximum period of enforcement of claims (3 years general limitation period).

Access: the personal data processed for complaint handling purposes may primarily be accessed by the Data Controller.

Data transfer: personal data will not be transferred to third parties, unless otherwise provided for in the contract between the data subject and the Data Controller.

Technique of data processing: the Data Controller processes the personal data of the data subject electronically.

Profiling: the Data Controller does not make decisions based solely on automated data processing in relation to the data subject, nor does it create a profile about the data subject based on the available personal data.

Rights of data subjects: in connection with data processing, data subjects may exercise the rights of access, rectification, erasure, restriction of processing and objection.

INFORMATION ON THE USE OF COOKIES

In accordance with common practice, the Data Controller also uses cookies on its website. Cookies alone are not suitable for identifying the user.

Cookies are small data files that are placed on the user's computer by the visited website.

The purpose of cookies is to ensure the continuous operation of the given info communication and internet service, to make it easier, more convenient and to contribute to the further development of the website with anonymous statistics.

There are many types of cookies, but they can generally be divided into two broad groups: one is the temporary (strictly necessary) cookie, which is placed on the user's device by the website only during a specific session (e.g. a single visit to the website); Another type is a persistent cookie (e.g. language setting of a website), which remains on the computer until the user deletes it. The Data Controller uses only temporary, strictly necessary cookies on its website. They are valid only for the duration of the visit. The Data Controller receives automatically generated information about the visitors of its website for the strength of the visit: the internet protocol (IP address) of the visitor, the time of the visit, the data of the pages viewed, the name of the browser used.
You can check what types of cookies the Data Controller's website uses on the following website: https://www.cookieserve.com/

Set up your browser

Accepting and enabling cookies is not mandatory. You can reset your browser settings to reject all cookies or notify you when a cookie is being sent, but some features or services may not work properly without cookies. Most browsers automatically accept cookies by default, but these can usually be changed to prevent automatic acceptance and offer you the choice each time.
The settings options are usually located in the "Options" or "Settings" menu of the browser, it is recommended to use the "Help" menu of the search engine for the settings that are most suitable for the data subject.

Scope of personal data processed: internet protocol address (IP address) of the visitor, time of visit, data of pages viewed, name of browser used.

Categories of data subjects: visitors to the Data Controller's website.

The source of the personal data processed is the data subject.

The purpose of data processing: to ensure the highest possible quality operation of the website visit.

Legal basis for data processing: consent of the data subject pursuant to Article 6 (1) (a) of the GDPR.

Duration of data processing: duration of a given visit.

Access: the processed personal data may primarily be accessed by the Data Controller.

Data transfer: the personal data of the data subjects are not transmitted by the Data Controller.

Technique of data processing: the Data Controller processes the personal data of the data subject electronically.

Profiling: the Data Controller does not make decisions based solely on automated data processing in relation to the data subject, nor does it create a profile about the data subject based on the available personal data.

Rights of data subjects: in connection with data processing, data subjects may exercise the rights to withdraw consent, access, rectification, erasure, restriction of processing, data portability.

DATA PROCESSING ON THE WEBSITE

The Data Controller informs the data subjects that it uses Google Analytics to measure the number of visitors and the behavior of its visitors and to compile statistics for measuring the total number of services and subpages available under the internet site domain name operated by it, and for compiling statistics, the corresponding codes of which it has integrated into its own site.

The linked programs place so-called cookies on the user's computer, which collect user data. Visitors to the website (Users) allow the Data Controller to use the Google Analytics program.

At the same time, they consent to the monitoring and tracking of their user behavior and to the use of all services provided by the programs to the Data Controller.

In addition, the user has the option to disable the recording and storage of cookies at any time with effect for the future.

Data subjects can find the settings and privacy notices for the use of Google Analytics on the Google website. https://policies.google.com/privacy?hl=hu

According to Google, Google Analytics mainly uses first-party cookies to report visitor interactions on your site. These cookies only record non-personally identifiable information.

Browsers do not share first-party cookies across domains. More information about cookies can be found in our Google Ads & Privacy FAQ.

Google Analytics: The Data Controller uses Google Analytics primarily to generate its statistics, including measuring the effectiveness of its website campaigns. By using the program, the Data Controller mainly obtains information about how many visitors visited its Website and how much time the 3 visitors spent on the Website.
The program recognizes the visitor's IP address, so it can track whether the visitor is a returning or a new visitor, and it can track the visitor's journey through the Website and where they have entered.

Scope of personal data processed: IP address, clicks

Categories of data subjects: visitors to the Data Controller's website.

Source of processed personal data: the data subject.

Purpose of data processing: promotion of the Data Controller's website and services, measurement of visits.

Legal basis for data processing: consent of the data subject. Article 6 (1) (a) GDPR.

Duration of data processing: 30 days.

Access: Google may access the personal data processed.

Data transfer: the personal data of the data subjects are not transmitted by the Data Controller.

Technique of data management: the Data Controller processes the processed personal data electronically.
Profiling: the Data Controller does not make decisions based solely on automated data processing in relation to the data subject, nor does it create a profile about the data subject based on the available personal data.

Rights of data subjects: in connection with data processing, data subjects may exercise the rights to withdraw consent, access, rectification, erasure, restriction of processing, data portability.

PROCESSING OF SENSITIVE DATA QUALIFYING PURSUANT TO ARTICLE 9 (1) GDPR

The Data Controller does not request special data from the data subject (racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, as well as data concerning health or sex life), so the Data Controller does not call the data subject to provide such data either by letter, telephone or in person.

Special data may be provided in a job application, complaint or comment submitted by the data subject to the Data Controller, but the provision of data depends on the voluntary decision of the data subject in this case as well, i.e. its provision is not mandatory.

If, nevertheless, the data subject decides that, for any reason, he or she considers it important to provide detailed information and thus sensitive personal data to the Data Controller, the legal basis for data processing is the consent of the data subject given after prior information pursuant to Article 6 (1) (a) GDPR, taking into account Article 9 (2) (a) GDPR.

If, notwithstanding the above, the data subject provides special data to the Data Controller, the Data Controller shall always return the original document containing such data to the data subject, without

making a copy thereof. An exception to this is if the data subject sends a letter and makes the sensitive data known to the Data Controller in the body of the letter.

SECURITY

The Data Controller and the data processors are entitled to access the personal data of the data subject only and exclusively to the extent necessary to perform tasks falling within their responsibilities.

The Data Controller shall carry out the transfer of personal data in a uniform, pre-audited manner, in a secure form, informing the data subject, avoiding redundant data transfer or disclosure on different registration interfaces.

In order to ensure data security, the Data Controller assesses and records all data processing activities performed by it.

Based on the records of data processing activities, the Data Controller performs a risk analysis in order to assess the conditions under which each data processing takes place, and which risk factors may cause what extent harm and what possible data protection incident during data processing. The risk analysis shall be carried out on the basis of the actual data processing activity carried out. The purpose of risk analysis is to determine security rules and measures that effectively ensure adequate protection of personal data in accordance with the performance of the Data Controller's activity.

Taking into account the nature, scope, context and purposes of the processing and the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Data Controller shall implement appropriate technical and organizational measures to ensure and demonstrate that the processing of personal data is carried out in accordance with the GDPR. This includes, inter alia, where appropriate:

- pseudonymisation and encryption of personal data;
- ensuring the continued confidentiality, integrity, availability and resilience of systems and services used for processing personal data;
- the ability to restore access to and availability of personal data in a timely manner in the event of a physical or technical incident;
- a procedure for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures taken to ensure the security of processing.

When determining the appropriate level of security, explicit account should be taken of the risks arising from processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

The Data Controller shall implement appropriate technical and organizational measures to ensure that, by default, only personal data that are necessary for the specific purpose of processing are processed. This obligation applies to the amount of personal data collected, the extent of their processing, the duration of their storage and their accessibility. In particular, those measures should ensure that, by default, personal data are not made available to an indefinite number of persons without the intervention of the natural person.
In the event of damage or destruction of personal data, attempts shall be made to replace the damaged data to the extent possible from other available data sources. The replacement data shall be indicated on the data.

The Data Controller protects its internal network with multi-level firewall protection. At the entry points of the public networks used, hardware firewalls (border protection devices) are always located

everywhere. The Data Controller stores the data redundantly – i.e. in several places – to protect them from destruction, loss, damage and unlawful destruction due to the failure of the IT device.

It protects your internal networks from external attacks with multi-level, active, complex malware protection (e.g. antivirus).

The Data Controller shall do everything possible to ensure that its IT tools and software continuously comply with the generally accepted technological solutions in market operation.

RIGHTS OF THE DATA SUBJECT

It is important for the Data Controller that its data processing complies with the requirements of fairness, legality and transparency. In connection with data processing, the data subject may at any time:

- request information about data processing and access to data processed concerning him,
- request rectification or completion of incomplete data in case of inaccurate data,
- request the deletion of data processed on the basis of your consent,
- object to the processing of your data,
- request restriction of processing.

Based on the request for information – if it is not restricted due to a statutory interest – you may find out whether your personal data are being processed by the Data Controller and you have the right to be informed in connection with the data processed concerning you that:

- for what purpose it is handled,
- what authorizes you to process the data (legal basis),
- from when and for how long you process your data (duration),
- what data it processes and provides a copy thereof to the data subject,
- the recipients or categories of recipients of the personal data,
- transfer to a third country or international organisation,
- if they were not collected from the data subject, the source of the data,
- the characteristics of automated decision-making, if used by the controller,
- your rights as a data subject related to data processing,
- legal remedies.

The Data Controller shall respond to requests for information and access within 25 days at the latest. For further copies of the personal data processed concerning the data subject, the Data Controller may charge a reasonable fee based on administrative costs.

If the correction (modification) of the data is requested, the data subject must prove the reality of the data requested to be modified, and he must also prove that it is indeed the authorized person who requests the modification of the data. Only in this way can the Data Controller judge whether the new data is real and, if so, whether it can modify the old one.

If it is not clear whether the processed data is correct or accurate, the Data Controller does not rectify the data, but only marks it, i.e. indicates that it was objected to by the data subject, but it may not be incorrect. After confirming the authenticity of the request, the controller shall, without undue delay, rectify the inaccurate personal data or complete the data concerned by the request. The Data Controller shall notify the data subject of the correction or designation.

If the deletion or blocking of data is requested, the data subject may request the deletion of his or her data, which means that the Data Controller is obliged to delete the data relating to the data subject without undue delay if:

- the personal data have been unlawfully processed
- the personal data are no longer necessary in relation to the purposes for which they were processed,
- if the processing of the data was based on the consent of the data subject and he or she has withdrawn it and another legal basis does not make the further processing lawful,
- the law requiring the Data Controller to erase the data imposes such an obligation and has not yet complied with it.

You may request the restriction of processing, which the controller will comply with if one of the following applies:

- the accuracy of the personal data is contested by the data subject, in which case the restriction applies for a period enabling the controller to verify the accuracy of the personal data,
- the processing is unlawful and the data subject opposes the erasure of the data and requests the restriction of their use instead,
- the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims; or against data processing concerning him.

Where data have been restricted, such personal data shall, with the exception of storage, only be processed with the consent of the data subject or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State. The Data Controller shall inform the data subject in advance of the lifting of the restriction of processing.

If the data subject considers that the data processing violates the provisions of the GDPR or considers the way in which the Data Controller processes his or her personal data to be infringed, we recommend that he or she first contact the Data Controller with his complaint. Your complaint will always be investigated.
If, despite your complaint, you still complain about the way the Data Controller processes your data or you would like to contact an authority directly, you may file a complaint with the Data Protection Authority: Data Protection Commission (address: 21 Fitzwilliam Square South, Dublin 2, D02 RD28, Ireland, website: https://www.dataprotection.ie/en).

You also have the option to go to court to protect your data.

Annex 1

Concepts relating to the processing of personal data

- controller: the legal entity that determines the purposes and means of the processing of personal data;
- processing: any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
- data transfer: making data available to a specific third party;
- data erasure: making data unrecognizable in such a way that their recovery is no longer possible;
- data marking: identification of the data in order to distinguish it;
- restriction of processing: marking of stored personal data with a view to limiting their processing in the future;
- data destruction: complete physical destruction of the data medium containing the data;
- data processor: a legal person that processes personal data on behalf of the controller;
- recipient: a natural or legal person, public authority, agency or any other body, to which the personal data are disclosed, whether a third party or not;
- data subject: an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;
- third party: a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;
- consent of the data subject: any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;
- personal data: any information relating to the data subject;
- objection: the statement of the data subject by which he objects to the processing of his or her personal data and requests the termination of data management or the deletion of the processed data.