

EU Data Act (EUDA) Pre-Sales Information Notice & Use Terms

1. Overview

- 1.1. This Information Notice (“Notice”) and the related Use Terms (these “**EUDA Terms**”) explain what Data is generated by PR Industrial s.r.l.’s and its subsidiaries and affiliates’ (“PRI”, “we”, “our”, “us”, or “**Data Holder**”) Connected Products and Related Services. They govern what Data can be accessed or shared, how to access it, and any conditions that apply. They implement the EU Data Act (Regulation (EU) 2023/2854), which entered into force 11 January 2024 and applies from 12 September 2025 (“EU Data Act”). We update the Notice and Use Terms from time to time to reflect the launch of new Products and features.
- 1.2. **By continuing, you acknowledge that you have read, understood and accepted these EUDA Terms.**

2. Parties

- 2.1. These **EUDA Terms** are between PR Industrial s.r.l. and the user of the Connected Product and/or who receives the Related Service(s) (“User”, “your”, or “you”). The User may be an owner, lessee, renter, or other lawful user of the Connected Product and/or who receives the Related Service(s).

3. Scope

- 3.1. If the User uses or receives the Data Holder’s Connected Products or Related Services in the European Union, the User has the right to access the Raw Data and Pre-Processed Data generated by the User’s use and to share that Data with a chosen third-party User. This obligation applies to Data that is readily available to the Data Holder.
- 3.2. Highly enriched or inferred Data and most content files (e.g., User-generated media) are typically out of scope.
- 3.3. For the avoidance of doubt, these EUDA Terms do not apply if the User is located outside the EU.

4. Definitions and Interpretation

- 4.1. The defined terms are set out in **Annex I-1** to these EUDA Terms. Capitalized terms not otherwise defined herein shall have the meaning given to them in the Agreement between PR and the User.

5. Data Generation & Storage Location

- 5.1. Our products and services generate different types of Product Data and Related Service Data depending on model and configuration.
- 5.2. We store Data either on local devices (for diagnostics and immediate access) or on secure servers located in European Union, with retention periods that depend on the dataset and purpose and comply with applicable law.
- 5.3. Annex I-1 outlines Product Data and Related Service Data details.

6. User’s Data Access Right

- 6.1. Upon receipt of a Data access request from the User and subject to clauses 7.4 to 7.6, Data Holder shall make readily available Data (and the relevant metadata necessary to interpret and use such Data), accessible to the User without undue delay, of the same quality as is available to the Data Holder, easily, securely, free of charge, in a comprehensive, structured, commonly used and machine-readable format and, where relevant and technically feasible, continuously and in real-time.
- 6.2. The request referred to in clause 6.1 may be submitted via email to privacy@pramac.com

- 6.3. The User may access the Data as follows: contact privacy@pramac.com. We will verify your identity and entitlement.
- 6.4. The Data Holder may restrict or prohibit accessing, using or further sharing the Data, if such processing could undermine the security requirements of the Connected Product, resulting in a serious adverse effect on the health, safety or security of natural persons.
- 6.5. The User shall provide the Data Holder with any information reasonably requested by the Data Holder that is necessary to verify the identity of the User and its entitlement to access the Data.
- 6.6. Where the Data constitute trade secrets or are protected as trade secrets, no Data will be disclosed unless the:
 - 6.6.1. User undertakes to preserve the confidentiality of the trade secrets and
 - 6.6.2. Data Holder and User will take all necessary measures prior to the disclosure to preserve the confidentiality in particular regarding third parties, including but not limited to proportionate technical and organisational measures necessary to preserve the confidentiality of the shared data, in particular in relation to third parties, such as model contractual terms, confidentiality agreements, strict access protocols, technical standards and the application of codes of conduct.
- 6.7. The User will implement and maintain the measures pursuant to clause 8 (“Trade Secret Protection Measures”). If User fails to implement or maintain such measures or undermines the measures or the confidentiality of the trade secrets, Data Holder may withhold or suspend the sharing of Data identified as trade secrets.
- 6.8. Where Data Holder is highly likely to suffer serious economic damage from the disclosure of trade secrets, despite the technical and organisational measures taken by User pursuant to clause 7.6, Data Holder may refuse on a case-by-case basis a request for access to the specific Data in question.
- 6.9. Where the Data in question constitutes personal data and User is not the data subject whose personal data is requested:
 - 6.9.1. any personal data generated by the use of the Connected Product or the Related Service shall be made available by the Data Holder to the User only where there is a valid legal basis for processing under Article 6 of the GDPR and, where relevant, the conditions of Article 9 of that Regulation and of Article 5(3) of Directive 2002/58/EC are fulfilled.
 - 6.9.2. The User shall specify the applicable legal basis for processing in each request submitted to the Data Holder; and where the Data may include personal data relating to the User’s employees, the User shall:
 - 6.9.2.1. ensure that the data subject is appropriately informed of the specific, explicit and legitimate purposes for processing such Data, and how the data subject may exercise their rights effectively; and
 - 6.9.2.2. provide the Data Holder with a legal declaration in the form as the Data Holder may provide.
- 6.10. If a legal basis is not appropriately identified, the Data Holder may either refuse or comply with the request referred to in clause 7.1 by anonymising the Data or, where the Readily Available Data contains personal data of several data subjects, transmitting only personal data relating to the requesting User (if that User is a data subject).

7. Other Access

- 7.1. We do not collect data for products which are not registered and connected to any of the device management services outlined below, so you will not be able to access data for these products other than contacting via email privacy@pramac.com.

8. User's Data Sharing Right

- 8.1. Upon User's request submission, or by a party acting on behalf of the User, Data Holder shall make available Readily Available Data, as well as the relevant metadata necessary to interpret and use such Data, to a third party data recipient without undue delay, of the same quality as is available to the Data Holder, easily, securely, free of charge to the User, in a comprehensive, structured, commonly used and machine-readable format and, where relevant and technically feasible, continuously and in real-time. Notwithstanding the foregoing, Data Holder shall have no obligation to share Data with third parties based outside the EU.
- 8.2. The Data Holder may charge the third-party data recipient for a non-discriminatory and reasonable compensation before making the Data available to the third-party data recipient.
- 8.3. Any request referred to in clause 8.1, including a request to terminate further Data sharing, may be submitted via privacy@pramac.com.
- 8.4. The Data Holder may restrict or prohibit accessing, using or further sharing Data, if such processing could undermine the security requirements of the Connected Product, resulting in a serious adverse effect on the health, safety or security of natural persons
- 8.5. The User, or any party acting on behalf of the User, shall provide the Data Holder with any information reasonably requested by the Data Holder that is necessary to verify both the identity of the User, the authority granted to such party by the User and the entitlement to access the Data.
- 8.6. Where the Data constitute trade secrets or are protected as trade secrets, such Data shall be disclosed to third parties only to the extent that such disclosure is strictly necessary to fulfil the purpose agreed between the User and the third-party data recipient. Notwithstanding the foregoing, no Data shall be disclosed unless the:
 - 8.6.1. third party data recipient undertakes to preserve the confidentiality of the trade secrets; and
 - 8.6.2. Data Holder and the third party data recipient agree to take all necessary measures prior to the disclosure to preserve the confidentiality in particular regarding third parties, including but not limited to proportionate technical and organisational measures necessary to preserve the confidentiality of the shared Data, in particular in relation to third parties, such as model contractual terms, confidentiality agreements, strict access protocols, technical standards and the application of codes of conduct.
- 8.7. The third-party data recipient shall implement and maintain measures that are no less restrictive than those imposed on the User under clause 8 ("Trade Secret Protection Measures"). If the third-party data recipient fails to implement or maintain such measures or undermines the measures or the confidentiality of the trade secrets, Data Holder may withhold or suspend the sharing of Data identified as trade secrets.
- 8.8. Where Data Holder is highly likely to suffer serious economic damage from the disclosure of trade secrets, despite the technical and organisational measures taken by the third-party data recipient pursuant to clause 8.6, Data Holder may refuse on a case-by-case basis a request for access to the specific Data in question.
- 8.9. For the avoidance of doubt, any failure on the part of Data Holder and third-party data recipient to agree on arrangements for transmitting the Data shall not hinder, prevent or interfere with the exercise of the rights of the data subject under the GDPR and, in particular, with the right to data portability under Article 20 of that Regulation.
- 8.10. Where the Data in question constitutes personal data and User is not the data subject whose personal data is requested:
 - 8.10.1. any personal data generated by the use of the Connected Product or the Related Service shall be made available by Data Holder to the third-party data recipient only where there is a valid legal basis for processing under Article 6 of the GDPR and, where relevant, the conditions of Article 9 of that Regulation and of Article 5(3) of Directive 2002/58/EC are fulfilled and
 - 8.10.2. where the Data may include personal data relating to the User's employees, User shall:

- 8.10.2.1. ensure that the data subject is appropriately informed of the specific, explicit and legitimate purposes for processing such Data, and how the data subject may exercise their rights effectively; and
 - 8.10.2.2. provide the Data Holder with a legal declaration in the form as the Data Holder may provide.
- 8.11. If a legal basis is not appropriately identified, the Data Holder may either refuse or comply with the request referred to in clause 9.1 by anonymising the Data or, where the Readily Available Data contains personal data of several data subjects, transmitting only personal data relating to the requesting User (if that User is a data subject).
- 8.12. The User agrees and confirms that any undertaking designated as a gatekeeper, pursuant to Article 3 of Regulation (EU) 2022/1925, shall not be an eligible third-party data recipient under this clause 5 and therefore shall not:
 - 8.12.1. solicit or commercially incentivise the User in any manner, including by providing monetary or any other compensation, to make Data available to one of its services that the User has obtained pursuant to a request under clause 6.1;
 - 8.12.2. solicit or commercially incentivise the User to request the Data Holder to make Data available to one of its services pursuant to clause 8.1;
 - 8.12.3. receive Data from the User that the User has obtained pursuant to a request under clause 6.1.
 - 8.12.4. contact if via the contact details below detailing the recipient and data sharing purpose.
- 8.13. Where Data Holder makes use of User Data itself, this is noted in PRI Privacy Notice and in the terms and conditions of the relevant digital service, such as Pramac EMS. Should User have any questions or require further assistance regarding data access User may contact Data Holder customer support team via: privacy@pramac.com.
- 8.14. User may raise any concerns by contacting:
 - 8.14.1. Data Holder using the customer support contact details for the device management services set out above to make a complaint relating to the Data Act in general.
 - 8.14.2. User's Member State's designated authority for Data Act enforcement. Each EU Member State has designated one or more competent authorities to be responsible for the enforcement of the Data Act. User may also lodge a complaint with the relevant competent authority in the EU Member State of User's habitual residence.

9. Trade Secret Protection Measures

- 9.1. Where User receives Data from the Data Holder or shares it with any third party data recipient and that Data contains trade secrets of Data Holder or its Affiliates, User will safeguard it against unauthorised access, use, or disclosure and to implement and maintain appropriate technical and organisational measures to preserve the confidentiality and secrecy of such Data. These measures shall include, at a minimum:
 - 9.1.1. limiting access to individuals within the User's household or organisation who have a legitimate need to use, access, or receive such trade secrets;
 - 9.1.2. informing any recipients of the confidential and proprietary nature of the trade secrets, and ensuring they are subject to equivalent obligations to maintain confidentiality and restrict use and access;
 - 9.1.3. adopting any additional safeguards that are necessary and proportionate to preserve the secrecy of the trade secrets, which may include confidentiality agreements, strict access protocols, technical standards and/or the application of codes of conduct (collectively referred to as "**Trade Secret Protection Measures**").

- 9.2. User shall not alter or remove any Trade Secret Protection Measures without prior written consent from the Data Holder. If the existing measures are deemed insufficient or inadequate to protect the trade secrets, Data Holder reserves the right to:
 - 9.2.1. unilaterally introduce, modify, or enhance any Trade Secret Protection Measures it applies, provided such changes do not materially impair the User's ability to access or use the Data; and
 - 9.2.2. require the User to implement additional safeguards necessary to ensure continued protection of the trade secrets.
- 9.3. User shall promptly notify the Data Holder of any event or circumstance that could reasonably be expected to compromise the confidentiality or secrecy of any trade secrets. User shall take all reasonable steps to:
 - 9.3.1. prevent such circumstances from arising;
 - 9.3.2. mitigate the impact of any such event; and
 - 9.3.3. restore the confidentiality and secrecy of the affected trade secrets.
- 9.4. Upon termination of these EUDA Terms pursuant to clause 22 ("Termination"), or when the trade secrets are no longer required, the User will securely destroy or permanently delete all such information.

10. Unauthorised Use or Sharing of the Data

- 10.1. The User may use the Data made available by the Data Holder for any lawful purpose and/or share such Data provided that the User shall not:
 - 10.1.1. use the Data obtained pursuant to a request referred to in clause 6.1 to develop a connected product that competes with the Connected Product or the Related Service from which the Data originate, nor share the Data with a third party data recipient with that intent;
 - 10.1.2. use the Data to derive insights about the economic situation, assets and production methods of the manufacturer or, where applicable the Data Holder;
 - 10.1.3. use coercive means or abuse gaps in the technical infrastructure of the Data Holder which is designed to protect the Data in order to obtain access to Data;
 - 10.1.4. share the Data with a third party considered as a gatekeeper under Article 3 of Regulation (EU) 2022/1925;
 - 10.1.5. use or share the Data for any purposes that infringe EU law or applicable national law; or
 - 10.1.6. use, disclose or share any Data that constitute trade secrets or are protected as trade secrets in a manner not compliant with these EUDA Terms.

11. Data Use and Sharing by the Data Holder

11.1. Use by the Data Holder

- 11.1.1. Data Holder may use any Readily Available Data that is non-personal Data solely for the purposes agreed with the User, which include, but are not limited to:
 - 11.1.1.1. providing, maintaining, improving, upgrading and enhancing our products and services;
 - 11.1.1.2. performing obligations under any agreement with the User, as well as executing related operational activities;
 - 11.1.1.3. ensuring the ongoing performance, safety, security, and integrity of the Connected Product or any Related Service, and conducting quality assurance activities;
 - 11.1.1.4. preventing, detecting, and investigating security incidents;
 - 11.1.1.5. delivering customer support, warranty or guarantee services, and evaluating claims made by the User, the Data Holder, or third parties;
 - 11.1.1.6. refining and optimizing the functionality of existing products and services provided by the Data Holder;
 - 11.1.1.7. developing new products and services either directly by the Data Holder, through third parties acting on its behalf, or in collaboration with other entities;

- 11.1.1.8. complying with an order of any court of competent jurisdiction or any regulatory, judicial, governmental or similar body or any taxation authority of competent jurisdiction; or the laws, regulations, rules or codes of any country to which the Data Holder is subject;
- 11.1.1.9. combining non-personal Data with other datasets or generating derivative Data for lawful uses. This may include making such Data available to third parties, provided it cannot be traced back to specific transmissions from the Connected Product or reverse-engineered to identify individual data points; and
- 11.1.2. Data Holder may use any Readily Available Data that is non-personal Data solely for such other purpose as may be permitted under applicable law, provided that the Data Holder shall not use such Readily Available Data that is non-personal Data to derive insights about the economic situation, assets and production methods of, or the use by the:
 - 11.1.2.1. User in any other manner that could undermine the commercial position of the User on the markets in which the User is active; and
 - 11.1.2.2. third-party data recipient in any other manner that could undermine the commercial position of the third-party data recipient on the markets in which the third-party data recipient is active, unless the third-party data recipient has given permission to such use and has the technical possibility to easily withdraw that permission at any time.

11.2. Sharing by the Data Holder to a Third-Party

- 11.2.1. Data Holder may share with third-party data recipient the Data, which is non-personal data, if the Data is used by the third-party data recipient exclusively for:
 - 11.2.1.1. fulfilment of any contract with the User; and
 - 11.2.1.2. assisting the Data Holder in achieving the purposes permitted under clause 11.1.
- 11.2.2. The Data Holder shall contractually bind the third-party data recipient to:
 - 11.2.2.1. process the Data made available to it only for the purposes and under the conditions agreed with the User and subject to EU and national law on the protection of personal data including the rights of the data subject insofar as personal data are concerned;
 - 11.2.2.2. erase the Data when they are no longer necessary for the agreed purpose, unless otherwise agreed with the User in relation to non-personal data;
 - 11.2.2.3. implement and maintain measures that are no less restrictive than those imposed on the User under clause 9; and
 - 11.2.2.4. *not* further share the Data received from the Data Holder unless the User grants general or specific agreement for such further transfer, or unless such Data sharing is required, in the interest of the User, to fulfil these EUDA Terms or any contract between the third-party data recipient and the User; and
 - 11.2.2.5. to observe and perform the obligations required under the EU Data Act.

11.3. Personal Data

- 11.3.1. Where the Data is or contains personal data, Data Holder may use, share with third-party data recipient or otherwise process such Data, under a legal basis provided for and under the conditions permitted under the GDPR and, where relevant, Directive 2002/58/EC (Directive on privacy and electronic communications).

12. Transfer of Use

- 12.1. Where the User sells or otherwise transfers to another person ("**New User**") (i) ownership of the Connected Products, (ii) its right to use the Connected Products, and/or (iii) its right to receive the Related Services, the User undertakes to:

- 12.1.1. terminate all live data access and request;
 - 12.1.2. disconnect the Connected Products and the Related Services from the User's account;
 - 12.1.3. ensure that the New User cannot use or access the User's account; and
 - 12.1.4. notify the Data Holder for deregistration.
- 12.2. Upon completion of the disconnection from the Connected Products and the Related Services, User will cease to be a user of those Connected Products and the Related Services.
- 12.3. Notwithstanding the foregoing, Data Holder shall be entitled to use any Data generated, collected or recorded prior to the transfer.

13. Additional Users

- 13.1. Where User grants another person ("**Additional User**") a right to use of the Connected Product and/or to receive the Related Service(s) while retaining its status as a User, the Data Holder will not be able to verify the Additional User's rights under the EU Data Act. The User undertakes to:
- 13.1.1. ensure that each Additional User agrees to these EUDA Terms, in particular clauses 6, 6, 9, 10, 11 and 12;
 - 13.1.2. ensure that each Additional User cannot use the User's account;
 - 13.1.3. act as the point of contact in relation to all data access or sharing request from the Additional User;
 - 13.1.4. verify each Additional User's right to the Data;
 - 13.1.5. before making any data access or sharing request on behalf of a requesting Additional User, ensure that other Additional Users have given consent to the Data being accessed and/or shared with the requesting Additional User or a data recipient chosen by the requesting Additional User;
 - 13.1.6. where the requesting Additional User has asked for the Data to be shared with third party data recipient, obtain the requesting Additional User's consent to share the Data with that third party data recipient;
 - 13.1.7. make any data access or sharing request on behalf of the requesting Additional User only for the Data to which the requesting Additional User has rights; and
 - 13.1.8. keep all records of requests and consents and provide them to the Data Holder upon request.

14. Switching

- 14.1. The User shall be entitled to notify its decision to perform one or more of the following actions by providing a maximum prior written notice of two (2) months ("**Notice Period**") to the Data Holder:
- 14.1.1. switch to a different provider of data processing services, in which case the User shall provide the necessary details of that provider;
 - 14.1.2. switch to an on-premises ICT infrastructure; and
 - 14.1.3. erase its exportable data and digital assets.
- 14.2. Upon receipt of a request from the User to switch to a data processing service offered by a different provider of data processing services or to port all exportable data and digital assets to an on-premises ICT infrastructure, the Data Holder shall, without undue delay and in any event in a reasonable time ("**Transitional Period**"), to be initiated after the maximum Notice Period, during which the service contract remains applicable, undertake the following:
- 14.2.1. provide reasonable assistance to the User and third parties authorised by the User in the switching process;
 - 14.2.2. act with due care to maintain business continuity, and continue the provision of the functions or services under these EUDA Terms;
 - 14.2.3. provide clear information concerning known risks to continuity in the provision of the functions or services on the part of the source provider of data processing services; and

- 14.2.4. ensure that a high level of security is maintained throughout the switching process, in particular the security of the Data during their transfer and the continued security of the Data during the Retrieval Period in accordance with applicable EU or national law.
- 14.3. Where the Transitional Period is technically unfeasible, the Data Holder shall notify the User within reasonable time of the making of the switching request and shall duly justify the technical unfeasibility and indicate an alternative transitional period, which shall not exceed seven (7) months, and ensure service continuity throughout the alternative transitional period.
- 14.4. Without prejudice to clause 14.3, the User shall have the right to extend the Transitional Period once for a period that the User considers more appropriate for its own purposes.
- 14.5. The Data Holder shall erase all exportable data and digital assets generated directly by the User, or relating to the User directly, after the expiry of the Retrieval Period or after the expiry of an alternative agreed period at a date later than the date of expiry of the Retrieval Period, provided that the switching process has been completed successfully.
- 14.6. The Data Holder will support the User's exit strategy relevant to the contracted services, including by providing all relevant information.
- 14.7. The User acknowledges and agrees that the Data Holder may impose switching charges in accordance with applicable EU law, including the EU Data Act, or national law.

15. Acceptance

- 15.1. The User's purchase or use of the Connected Product and/or the Related Service shall constitute the User's acceptance of these EUDA Terms.

16. Warranties and Representations

- 16.1. The User represents and warrants that User either owns the Connected Product, are contractually entitled to use it under a rent, lease, or similar agreement, or receive the Related Service(s) in connection with the Connected Product.

17. Further Undertakings

- 17.1. The User further undertakes to the Data Holder that:
 - 17.1.1. the User will provide to the Data Holder any relevant documentation to support the declarations the User has provided, where necessary and upon request;
 - 17.1.2. where the User is not the data subject whose personal data is requested, the User will provide a valid legal basis for processing under Article 6 of the GDPR and, where relevant, ensure that the conditions of Article 9 of that Regulation and of Article 5(3) of Directive 2002/58/EC are fulfilled;
 - 17.1.3. the User will enter into a contract with third party data recipient regarding the third-party data recipient's processing of the Data; and
 - 17.1.4. where a user alters or removes technical protection measures applied by the Data Holder or does not maintain the technical and organisational measures taken by the user in agreement with the Data Holder or, where they are not the same person, the trade secrets holder, in order to preserve trade secrets, as well as in respect of any other party that receives the Data from the user by means of an infringement of the EU Data Act, it shall comply, without undue delay, with the requests of the Data Holder to:
 - 17.1.4.1. erase the Data made available by the Data Holder and any copies thereof;
 - 17.1.4.2. end the production, offering or placing on the market or use of goods, derivative data or services produced on the basis of knowledge obtained through such Data, or the importation, export or storage of infringing goods for those purposes, and destroy any infringing goods, where there is a serious risk that the unlawful use of those Data will cause significant harm to the Data Holder, the trade secret holder or the User or where

such a measure would not be disproportionate in light of the interests of the Data Holder, the trade secret holder or the User;

- 17.1.4.3. inform the Data Holder of the unauthorised use or disclosure of the Data and of the measures taken to put an end to the unauthorised use or disclosure of the Data; and
- 17.1.4.4. compensate the party suffering from the misuse or disclosure of such unlawfully accessed or used Data.

18. Indemnification

- 18.1. The User shall indemnify, defend, and hold harmless each Indemnified Person from and against all claims and Losses incurred by any Indemnified Person(s) as a result of or in connection with any breach of clauses 6.5, 6.6, 6.7, 6.9, 8.5, 8.6, 8.6, 9, 10, 12, and 13.

19. Equitable Remedies

- 19.1. The User acknowledges and agrees that any breach or threatened breach of these EUDA Terms may result in irreparable harm for which monetary damages would be an inadequate remedy. Accordingly, the Data Holder shall be entitled to seek injunctive relief and specific performance, in addition to any other remedies available at law or in equity. Nothing in these EUDA Terms shall be construed to limit or restrict the Data Holder's right to pursue such equitable remedies.

20. Limitation of Liability

- 20.1. Nothing in this clause limits or excludes:
 - 20.1.1. liability for deliberate default;
 - 20.1.2. liability for death or personal injury caused by negligence;
 - 20.1.3. liability for fraud or fraudulent misrepresentation;
 - 20.1.4. liability under clause 18; or
 - 20.1.5. any liability that cannot legally be limited.
- 20.2. We make no warranty, representation or promise that:
 - 20.2.1. the Data will meet your requirements or expectations; or
 - 20.2.2. the Data will be available on an uninterrupted, timely, secure, vulnerability-free, virus-free or error-free basis.
- 20.3. Subject to clause 20.1, to the maximum extent permitted by applicable law:
 - 20.3.1. we disclaim and exclude all conditions, warranties, representations or other terms of any kind, express or implied, including, without limitation, those relating to quality, merchantability, fitness for a particular purpose, reasonable care and skill, reasonable time, usage, course of dealing, and non-infringement with respect to the Data, or that arise from a course of dealing, usage, or trade practice; and
 - 20.3.2. we shall not be liable to you in contract, tort (including negligence), breach of statutory duty, or otherwise for any direct, indirect, special, consequential, exemplary, punitive or incidental losses or damages (including, without limitation, loss of goodwill, reputation, profit, revenue, savings, contract, business opportunity or commercial opportunity, data, costs of replacement goods, or loss or damage to data, computer or system) resulting from, arising out of or in connection with the use or inability to use, sharing of, reliance on or any changes made to, the Data, even if we have been advised of the possibility of such losses or damages.
- 20.4. The User acknowledges, agrees and confirms that the Data Holder shall not be responsible for any Loss or damage which arises from or in connection with any breach of these EUDA Terms by the User.
- 20.5. The User further agrees and confirms that the Data Holder shall not be responsible for or held liable for (i) the User's choice of the third party data recipient,(ii) the absence of any contract between the User and any third party data recipient chosen by the User, and (iii) any claims, damages or losses arising from or in connection (i) or (ii).

- 20.6. In the event of any loss or damage to the Data, your sole and exclusive remedy shall be for the Data Holder to use reasonable commercial endeavours to restore the lost or damaged Data. The Data Holder shall not be responsible for any loss, destruction, alteration or disclosure of Data, howsoever and by whosoever caused.
- 20.7. Subject to clause 20.1, each Party's total liability for all claims and Losses arising from or connected with these EUDA Terms or any other contracts between the Parties shall not exceed €100.
- 20.8. Subject to clause 20.1, each Party may not bring more than one claim arising out of the same event, series of related events, or substantially similar circumstances. Multiple claims based on the same or similar facts shall be treated as a single claim for the purposes of calculating liability. Each Party shall not bring any claim, action, or proceeding arising out of or in connection with these EUDA Terms unless such claim is commenced within twelve (12) months from the date on which the cause of action first arose. For the avoidance of doubt, the cause of action shall be deemed to have arisen when the facts giving rise to the claim were, or ought reasonably to have been, known to it.

21. Term

- 21.1. For a user who purchases the Connected Product only, these EUDA Terms shall become effective on the date of the purchase ("**Product Effective Date**").
- 21.2. For a user who subscribes to the Related Service only, these EUDA Terms shall become effective on the date of subscription ("**Related Service Effective Date**").
- 21.3. Where a user purchases the Connected Product and subscribes to the Related Service, these EUDA Terms shall become effective on the earlier of the Product Effective Date or the Related Service Effective Date ("**Earlier Effective Date**", and collectively with the Product Effective Date and Related Service Effective Date, the "**Effective Date**").
- 21.4. These EUDA Terms shall remain in effect unless and until terminated in accordance with these EUDA Terms.

22. Termination

- 22.1. These EUDA Terms may be considered terminated in any of the following circumstances:
 - 22.1.1. where the User transfers the entire ownership of the Connected Product and discontinues use of the Related Service;
 - 22.1.2. upon the successful completion of the switching process;
 - 22.1.3. at the end of the maximum Notice Period, where the User does not wish to switch but to erase its exportable data and digital assets upon service termination;
 - 22.1.4. upon the destruction or permanent disposal of the Connected Product and discontinuation of the Related Service;
 - 22.1.5. where the User loses the right to use the Connected Product and the Related Service under a rental, lease or similar agreement;
 - 22.1.6. where these EUDA Terms is replaced by new terms; or
 - 22.1.7. in the event of a merger, acquisition, or sale of assets involving the Data Holder, where the successor entity does not assume the obligations under these EUDA Terms and new terms are entered into with the User.
- 22.2. Termination of these EUDA Terms shall not affect any rights, obligations, or liabilities under these EUDA Terms and applicable law that have accrued prior to the effective date of such termination.

23. Effect of Termination

- 23.1. Upon termination, User shall immediately cease to access or retrieve any Data generated, collected or recorded.

- 23.2. Notwithstanding the termination, User agrees and confirms that the Data Holder remains entitled to use and share the Data unless the User separately contacts the Data Holder to request the deletion of the relevant Product Data and Related Service Data.
- 23.3. Clauses 4, 8, 10, 11, 23, 16, 17, and 25 shall survive the termination of these EUDA Terms.

24. General Provisions

24.1. Notice

- 24.1.1. Any notice or other communication under or in connection with these EUDA Terms shall be in writing.
- 24.1.2. Notices from us to the User shall be sent by email to the email address provided by the User. The User shall ensure that the email address provided is current and accurate and promptly update us if it changes.
- 24.1.3. Notices from the User to us shall be submitted via email at privacy@pramac.com.
- 24.1.4. Any notice shall be deemed to have been received at the time of transmission if sent on a business day between 9:00 am and 5:00 pm in that jurisdiction, or, if this time falls outside normal business hours in that jurisdiction, then it is deemed received the following business day, at 9:00 am.
- 24.1.5. This clause does not apply to the service of any proceedings or other documents in any legal action or, where applicable, any arbitration or other method of dispute resolution.

24.2. Force Majeure

- 24.2.1. Neither Party shall be in breach of these EUDA Terms or otherwise liable for any failure or delay in the performance of its obligations if such delay or failure results from events, circumstances or causes beyond its reasonable control. The time for performance of such obligations shall be extended accordingly.

24.3. Communication, Complaints and Disputes

- 24.3.1. The User may contact the Data Holder via email at privacy@pramac.com.
- 24.3.2. In case of complaints or disputes, the Parties agree to use their best efforts to resolve the matter amicably.
- 24.3.3. Without prejudice to the User's right to lodge a complaint alleging an infringement of any provision of the EU Data Act with the competent authority designated pursuant to the EU Data Act and any other rights under the EU Data Act, the User agrees to submit complaints or concerns to the Data Holder via [this form](#) before bringing a case before any competent authority, court or tribunal.

24.4. Entire Agreement

- 24.4.1. These EUDA Terms contain the entire agreement between the Parties relating to the subject matter hereof and supersede all previous and contemporaneous agreements, arrangements and understandings between them, whether written or oral, relating to that subject matter.
- 24.4.2. Each Party acknowledges that, in entering into these EUDA Terms, it does not rely on any statement, representation, assurance or warranty (whether made negligently or innocently) of any person (whether a party to these EUDA Terms or not) ("**Representation**") other than as expressly set out in these EUDA Terms.
- 24.4.3. Each Party agrees that the only rights and remedies available to it arising out of or in connection with a Representation shall be for breach of contract.

24.5. Variation

24.5.1. The Parties agree that the Data Holder may amend these EUDA Terms from time to time, either at the sole discretion of the Data Holder or to reflect changes in applicable law.

24.5.2. The Data Holder shall provide the User with no less than one (1) month's prior notice of any such amendment, unless providing such notice would be impossible or unreasonable under the circumstances, or the amendment is required to ensure compliance with applicable law, in which case notice may be given as soon as reasonably practicable. The User's continued use of the Connected Product or the Related Service or access to the Data following the expiry of the notice period shall constitute acceptance of the amendment(s) and the updated terms of these EUDA Terms.

24.6. Severability

24.6.1. If any part or provision of these EUDA Terms is or becomes invalid, illegal or unenforceable, the validity, legality and enforceability of any other provision of these EUDA Terms shall not be affected and such part or provision may be modified to make these EUDA Terms as modified, valid, legal and enforceable. If such modification is not possible, the relevant part or provision of these EUDA Terms shall be deemed deleted. Any modification to or deletion of any part or provision of these EUDA Terms shall not affect the validity, legality and enforceability of the rest of these EUDA Terms.

24.7. Governing Law and Jurisdiction

24.7.1. These EUDA Terms are governed by and interpreted in accordance with the laws of Italy, without prejudice to the mandatory rights and protections afforded to the User under applicable laws, including the EU Data Act and relevant national laws of EU Member States.

24.7.2. The Parties irrevocably agree that the courts of Siena, Italy shall have exclusive jurisdiction to settle any disputes arising out of or in connection with these EUDA Terms, except where mandatory consumer protection laws or applicable EU legislation require otherwise.

Annex I-1

Definitions

Unless the context otherwise requires, the following terms shall have the meanings set out under these EUDA Terms:

“Affiliates”

means, with respect to either party, any person or entity that is directly or indirectly controlling, controlled by, or under common control with such party.

“Data”

means any Product Data and Related Service Data (including the relevant metadata necessary to interpret and use those data), the specifications and characteristics of which are set out in the Appendix, as may be amended from time to time. For the avoidance of doubt, the EU Data Act applies to the Data that are not substantially modified, meaning the Raw Data and the Pre-processed Data, the Data does not include:

- a. Data generated by a sensor-equipped connected product when the User records, transmits, displays or plays content, as well as the content itself, which is often covered by intellectual property rights, inter alia for use by an online service; and
- b. Data obtained, generated or accessed from a Connected Product, or transmitted to it, for the purpose of storage or other processing operations on behalf of any other party who is not the User.

“EU”

means European Union.

“EU Data Act”

means the Regulation (EU) 2023/2854, as amended, superseded or replaced from time to time.

“GDPR”

means the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regards to the processing of personal data and on the free movement of such data, as amended, superseded or replaced from time to time.

“Indemnified Persons”

means the Data Holder and each of its Affiliates and each of its and their directors, officers, employees, agents and licensees, and **“Indemnified Person”** means any of them;

“Losses”

means all liabilities, damages, losses (including loss of profits, loss of business, loss of reputation, loss of savings and loss of opportunity), fines, expenses and costs (including

all interest, penalties, legal costs (calculated on a full indemnity basis) and reasonable professional costs and expenses).

“Pre-processed Data”

means the Data which have been pre-processed for the purpose of making them understandable and useable prior to subsequent processing and analysis. The term “Pre-processed Data” should not be interpreted in such a manner as to impose an obligation on the Data Holder to make substantial investments in cleaning and transforming the data.

“Raw Data”

means the Data in raw form, also known as source or primary data which refer to data points that are automatically generated without any further form of processing.

Retrieval Period

means a minimum period for data retrieval of at least thirty (30) calendar days, starting after the termination of the Transitional Period or such alternative transitional period that was agreed between the User and the Data Holder;

“Connected

Products”, “Connected

Products

Data”, “exportable data”, shall have the meanings given to them in the EU Data Act.

“metadata”, “Readily

Available Data”, “Related

Service”, “Related Service

Data” and “User”

“data subject” and

“personal data”

shall have the meanings given to them in the GDPR.

Annex I-1 Details of the Data

Data Summaries

The table summaries below give a high-level indication of the sort of data you will find on each Product.

Data Volumes

The volume of data generated varies by product and related service and depends on usage. While it is not possible to complete detailed estimates for each product, we have provided some estimated approximate volume per user per day below to give users a sense of how much data their products generate.

Product type	Type of Data	Examples	Format	Estimated Volume / User / Day	Collection Frequency	Capable of generating data continuously and in real-time?	Capable of storing data on-device or on a remote server? Where?	Exportable	Retention Period	How the user may access, retrieve or, where relevant, erase the data
G8610	Device Info	LAN IP USB ID MAC address	NV stored	1 kB	IP – When edited USB ID, MAC, factory set	No	On-device	No	Life of the product	Using the Configuration Suite PC software or module UI

	Configuration file	Configuration of alarm levels Inputs/outputs selection Communication settings Splash screen User defined icons	Configuration file. downloaded	256kB when edited by the user	When changed by the user only	No, when user edited only	On device	Yes	Life of the product	Using the Configuration Suite PC software or DSE Assistant software or UI
	PLC file	User edited PLC rungs	Part of the configuration file	65 kB	When changed by the user only	No, when user edited only	On device	Yes	Life of the product	Using the Configuration Suite PC software or DSE Assistant software or UI
	Data logging	Instrumentation and alarms from real time operation	Data logging file	1MB on device or external memory available size	User set, max 1 second	Yes	Internal memory or external USB stick user provided	Yes	Life of the product	Using the Configuration Suite PC software

	Event Log	State machine changes Alarms	Event log file	512kB	Events driven	Yes	On device	Yes	Life of the product	Using the Configuration Suite PC software or module UI
	Language file	Customer set strings	Language file	128kB	When user edited	No	On device	Yes	Life of the product	Using the Configuration Suite PC software or module UI
	Accumulated data	Total runtime Total KWh Total KVAh Total rKVAh	NV stored data	128kB	When generator running	Yes	On device	No	Life of the product	Using the Configuration Suite PC software or module UI
Pramac Smart Energy Controller (PSEC), Pramac Energy Management	Local measurement readings, Device Info	Voltages, Currents, Power, Energy, Temperatures, Errors, Device Status, CPU	N/A. Real-time data	~250 MB/Site/Day	5s	Yes	Yes, locally (7 days) and within Cloud EMP (no limitation)	Yes	7 days local retention policy. No retention policy yet within Cloud EMP	Display data via local or Cloud UI, export function within Cloud Ui, local (Modbus TCP,

nt Platform (EMP)		Load, Fan Speed								REST API) and Cloud interfaces (REST API)
----------------------	--	--------------------	--	--	--	--	--	--	--	--