Personal Data Consent Policy

Revision History

Revision Date	Summary of Changes	Version	Updated By	Changes marked
11/8/2024	Initial draft	1.0	dstapleton	N
2/5/2025	Annual review with Marketing, minor edits	1.1	Dstapleton	N
5/22/2025	Re-classified prior to posting to Trust Center	1.2	Dstapleton	N

Document Properties

Status	Check Sharepoint for Status
Document Owner	Data Protection Officer (DPO)
Classification	Internal
Approval	Chief Technology Officer (CTO)
Distribution	All employees

ProcessUnity reviews all policies annually per the Policy Management Policy. Below is an excerpt from the Policy Management Policy regarding policy review, distribution, and acknowledgement.

Annual Review

All policies are reviewed annually by the executive management team for accuracy and required changes. All information security policies must be reviewed by the Vice President of Information Security, Chief Information Security Officer, or the Chief Technology Officer to identify and make any changes required to ensure that the policies remain consistent with business objectives and emerging threats and best practices. Following the annual review, the policies must be re-approved by the Vice President of Information Security, even if no changes are required.

Distribution and Acknowledgement

Applicable policies, along with any associated Standards, Guidelines, Processes, and Procedures, must be made available to all ProcessUnity Workers. ProcessUnity Workers will be informed of any policy changes. ProcessUnity Workers will be required to acknowledge, read, and agree to abide by each Policy as defined by the executive management team:

- Upon hire
- Upon policy change
- Annually

Table of Contents

1. Objective

This policy defines the requirements for ProcessUnity employees to obtain consent before collecting and processing personal data.

2. Purpose

2.1 This policy is intended as guidance for all ProcessUnity employees and contractors to enable compliance with applicable Data Protection Laws.

2.2 This policy applies to all personal data we process as a business, regardless of the media on which that data is stored or whether it relates to past or present employees, contractors, customers, clients or suppliers, shareholders, app or web users, or any other individual.

2.3 Failure to comply with the applicable Data Protection Laws puts both staff and ProcessUnity at risk, and so ProcessUnity takes compliance with this Policy seriously.

2.4 This Policy is aimed at all ProcessUnity staff members and it provides guidance how ProcessUnity relies on consent as a lawful basis for processing personal data for certain activities. Examples of the activities for which ProcessUnity relies on consent are set out in Appendix 1.

2.5 This policy considers:

2.5.1 what constitutes valid consent under applicable Data Protection Laws;
2.5.2 consent forms;
2.5.3 consent records;
2.5.4 withdrawing consent;
2.5.5 direct marketing; and
2.5.6 existing marketing/other databases.

2.6 ProcessUnity also processes personal data for existing and potential customers for its marketing activities (including event management and its website, including website analytics). In respect of these processing activities ProcessUnity relies on legitimate interests as a lawful basis for processing.

3. What constitutes valid consent

3.1 In order for ProcessUnity to rely on consent, the consent you have obtained from our existing and potential customers, job candidates, employees and others (the "Data Subject") must satisfy each of the following criteria:

3.1.1 Freely Given
This means that the Data Subject must have a genuine choice and must be able to refuse or withdraw consent. We must avoid bundling consent with other matters and keep it separate. Therefore, do not rely on blanket clauses in ProcessUnity's terms and conditions that request a blanket marketing consent. We should also avoid making consent to marketing conditional on our performance of a contract especially where consent is not required in order for us to provide a service to the data subject.

3.1.2 Specific
When you obtain marketing consent it is imperative that the consent must relate to the specific marketing purpose or purposes for which you are planning to use the consent. You must explain how you are planning to use the personal data and the

consent must be given in relation to those uses. General statements when obtaining consent must be avoided. In addition, if you are going to use the consent for other purposes, which were not disclosed when the consent was originally obtained, or if the purposes for which you originally obtained consent change, then you must go back and obtain consent for the new or changed purposes.

3.1.3 Informed

You must give the data subject all the necessary details of the processing activity in a language and form they can understand so that they can comprehend how the processing will affect them. For consent to be informed you must ensure that at the time you collect the consent ProcessUnity's identity and purposes of processing are made known to the data subject. Accordingly, you must state clearly that the Data Subject's personal data will be uploaded to our email marketing platform and will be used for sending emails relating to ProcessUnity's services.

3.1.4 Unambiguous

This means that an active indication of consent with a clear statement or affirmative action is required, if a Data Subject actively ticks a selection box that action will be considered unambiguous consent, whereas a pre-ticked box may not. Therefore, please refrain from using pre-ticked boxes when obtaining consent. Silence or pre-ticked boxes do not constitute unambiguous consent.

3.1.5 Refreshing Consent

Please ensure that consents which you have collected are refreshed at appropriate intervals. Providing all the information again to the Data Subjects to ensure that the data subjects remain well informed about how their personal data is being used and how to exercise their rights in relation to such consent.

4. Consent forms

4.1 Consent must be obtained before any personal data is processed for marketing purposes, or any other purposes for which consent is required under applicable Data Protection Laws (such as where we process special category data, a list of which is set out in Appendix 2).

4.2 You must ensure that all forms or requests for consent to collect and use personal data for marketing purposes allow the Data Subject to easily identify ProcessUnity as the data controller and to understand what he or she is agreeing to. The form must clearly describe the purpose or purposes for which the personal data is being collected.

4.3 We never obtain or rely on oral consent. Use of oral consent within ProcessUnity is strictly prohibited. If a Data Subject provides you with their business card, we regard the provision of the business card as written consent to process that data subject's personal data for marketing purposes.

4.4 Whether you are collecting personal data directly at marketing events or through mechanisms such as website forms or promotional forms, all such forms should contain the following minimum information and be expressed in clear and plain language which is easy for the Data Subject to understand:

4.4.1 the ProcessUnity legal entity's name, registered office address and company number;

4.4.2 the purpose, each of the marketing activities for which consent is being sought and specifically for the purpose of email marketing;

4.4.3 what type of personal data will be collected and utilised by ProcessUnity;

4.4.4 the existence of the right to withdraw consent, see paragraph 5 below;

4.4.5 the name and address of any multiple or joint controllers to whom personal data is to be transferred;

4.4.6 a link to the ProcessUnity privacy policy (at https://www.processunity.com/privacy-policy/);

4.4.7 if consent is being collected by electronic means for example through an online application form or websites, the request must be clear and concise;

4.4.8 do not use pre-ticked opt in boxes as, for example, these are invalid under European Data Protection Laws; and

4.4.9 ensure there is a consent declaration for the Data Subject to sign, this may include the use of a tick box or electronic signature which the Data Subject must tick or actively sign to signify the Data Subject's consent.

5. Consent records

5.1 You are obliged to ensure that if required, ProcessUnity can demonstrate that it has received consent from the data subject and prove that ProcessUnity has obtained valid consent from the Data Subject.

5.2 For all consents used by your department for processing personal data for marketing purposes you are required to set up a folder which contains all consent forms and records of consents which are easily linked to the Data Subjects whose personal data is being processed for marketing purposes.

6. Withdrawal of consent

6.1 You must ensure that at the time that you collect consent, the Data Subject is granted the right to easily withdraw consent at any given time.

6.2 Withdrawing consent should not be linked to any payment or be detrimental to the Data Subject.

6.3 If consent is withdrawn, you must stop processing the personal data.

6.4 Please keep a record of withdrawal of consent with the consent form and ensure it is recorded in all systems as required in order to ensure the personal data is not processed.

6.5 If you have another lawful basis for processing the personal data (such as legitimate interests) in respect of which consent has been withdrawn, you may process the personal data on the basis of the other lawful criteria. In order to continue to use the personal data on the other lawful criteria you must first inform the Data Subject.

7. Direct and automated marketing in the EU

7.1 If you have obtained personal data relating to Data Subjects in Europe from marketing lists, before using such personal data you must comply with the following requirements:

7.1.1 verify that the supplier of the list is one that has been approved by Marketing, or belongs to a professional body or holds an accreditation;

7.1.2 only use suppliers of lists where we have a contract with them to acquire the list which provides an indemnity to ProcessUnity for breach of European Data Protection Laws. The contract must also contain a provision which allows us to audit the supplier and how they obtained the list data;

7.1.3 the supplier must verify that the data subjects on the list:

(a) gave specific consent to receive marketing information from ProcessUnity;

(b) were provided with information as to how their information would be used with adequate privacy notices;

(c) were offered a clear and genuine choice whether or not to have their details used for marketing purposes;

(d) took positive action to indicate their consent; and

(e) agreed to receive marketing by texts, emails or automated calls where we will be using these methods to communicate with the data subjects.

7.1.4 the product or service we are marketing are the same or similar to those that the data subjects originally consented to receive marketing for;

7.1.5 only use the information on the lists for marketing purposes;

7.1.6 screen the data subjects on the list against our own lists to ensure that we do not contact data subjects who have told us they do not want our emails or calls;

7.1.7 review our lists to ensure that they are reliable;

7.1.8 include our name and contact details when marketing by post, email or call;

7.1.9 we are clear with the data subjects as to where we obtained their details; and

7.1.10 provide a copy of our relevant privacy policy.

7.2 Where you are going to market using physical mail, you must screen the names and addresses by the Mail Preference Service in the UK or other relevant mail screening service in Europe.

7.3 Where you are going to market using live phone calls, you must screen the numbers against the Telephone Preference Service in the UK (or for corporate subscribers against the Corporate Telephone Preference Service in the UK) or other relevant telephone screening service in Europe.

7.4 You must keep your own "do not call" list for anyone who indicates they do not wish to receive our calls. You must screen against our own "do not call" list. You must ensure our number is displayed to the person you are calling.

7.5 We do not process personal data using automated processing or other artificial intelligence systems for purposes such as the profiling of personal data.

8. Existing marketing/other databases

8.1 Where the ProcessUnity marketing or other department already stores personal data belonging to data subjects, you may continue to use that personal data provided that the consent you have previously obtained meets the standards for consent set out in this policy.

9. Data protection officer

9.1 The data protection officer (DPO) has the responsibility of ensuring effective oversight and management of ProcessUnity's data protection obligations. The DPO has access to the Board and to all of ProcessUnity's records, physical properties and personnel that are relevant to data processing and compliance.

9.2 The DPO sets the data protection policies and procedures for the company that explain how we comply with its data processing obligations on a day-to-day basis.

9.3 ProcessUnity's DPO is Dave Stapleton. He can be contacted at: privacy@processunity.com.

10. Questions

10.1 If you have any questions about this policy please contact ProcessUnity's Data Protection Officer.

11. Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

APPENDIX 1 – CONSENT AS PROCESSUNITY'S LAWFUL BASIS FOR PROCESSING

The following are examples of where ProcessUnity relies on consent as its lawful basis for processing personal data:

1. Marketing: direct marketing via email (for example, our Mailchimp or Hubspot email campaigns), mail (for example, where we do mailing campaigns using Reachdesk), or if we do any telephone marketing.

2. Recruitment/Human Resources: where we collect special category data relating to job candidates or employees, for example certain types of demographic data and health information (see Appendix 2).

APPENDIX 2 – SPECIAL CATEGORY DATA

The following is the list of "special category data".

If we were to process special category data (for any purpose), we must obtain the Data Subject's consent and keep a record of that consent.

- personal data revealing **racial or ethnic origin**;
- personal data revealing **political opinions**;
- personal data revealing **religious or philosophical beliefs**;
- personal data revealing **trade union membership**;
- **genetic data**;
- **biometric data** (where used for identification purposes);
- data concerning **health**;
- data concerning a person's **sex life**; and
- data concerning a person's **sexual orientation**.