D2.12
User protection processes and mechanisms 2.0
version 1.0

PUBLIC

Panagiotis Bouklis
European Dynamics S.A.
209, Kifissias Av. & Arkadiou Str.
15124 Maroussi
Athens

panagiotis.bouklis@eurodyn.com
+30 210 8094500

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 951813.

Project acronym	Project title	Grant agreement No.
Better Factory	Grow your manufacturing business	951813

Deliverable No.	Deliverable title	Version
D2.12	User protection processes and mechanisms 2.0	2.0

Type	Dissemination level	Due date
DEMONSTRATOR	PUBLIC	28.2.2023

Lead beneficiary	WP No.
ED	2

Main author	Reviewed by
Panagiotis Bouklis	Ruben Roex
Accepted by Project Coordinator	**Accepted by Technical Coordinator**
Magnus Simons	Ali Muhammad

Contributing author(s)	Pages
	20

VTT archive code	Lead beneficiary archive code
VTT-R-01391-20	

Abstract

RAMP provides a range of tools and functionalities which relate to the collaboration between different organisations and companies of the automation value chain, especially regarding the provision of services from different kinds of providers (automation technology, consultants, integrators, etc.) to manufacturing SMEs. As such, RAMP acts as the trusted intermediary between these companies. Additionally, the adoption of RAMP in the companies' activities is highly dependent on how much they trust that the platform goes beyond the technical aspect of protecting their data, but also that the services they receive are of high quality. This deliverable describes the mechanisms for protecting the users in using RAMP, beyond the technical aspect, as well as for enhancing their trust, with an ultimate goal of increasing the adoption of RAMP by the different actors of the automation value chain, i.e., manufacturing SMEs, automation technology providers, consultants, system integrators, robotics developers, etc.

Project Coordinator contact

Magnus Simons
VTT Technical Research Centre of Finland Ltd
Visiokatu 4, P.O. Box 1300, 33101 Tampere, Finland
E-mail: magnus.simons@vtt.fi
Tel: +358 40 543 8586

Technical Coordinator contact

Ali Muhammad
European Dynamics SA
E-mail: ali.muhammad@eurodyn.com
Tel: +358 400 560 851

Acknowledgement

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 951813

HISTORY OF CHANGES

Date	Version	Author	Comments
Xx/04/2023	**1.0**	**Panagiotis Bouklis**	**V1.0**

TABLE OF CONTENT

EXECUTIVE SUMMARY

From a legal and business perspective, trust within the RAMP ecosystem as well as the protection of RAMP users is crucial. From a legal perspective, implementing data protection measures and processes is often one of the important aspects that impacts trust and user protection. From a business perspective, however, processes that are aimed to increase the comfort and trust of users in using RAMP are also important.

Protection mechanisms in RAMP aim to ensure the following aspects:

- Confirmation / validation of transactions performed through RAMP
- Enhancement of the credibility of the companies, organizations and components in RAMP
- Protection of transactions taking place within RAMP
- Protection of the data and information shared within RAMP, and especially in the collaboration spaces
- Trust building for the data processing that takes place within RAMP
- Conflict resolution between RAMP companies
- Logging of actions and providing evidence of the occurrence of actions on RAMP

More specifically, in this version of the user protection and trust-enhancing mechanisms the following aspects are addressed:

- Transactions and collaboration between different organizations,
- Ensuring the credibility of companies that are registered in the RAMP, in terms of users being authorized to manage these companies' account and assuring their quality,
- Assuring the quality of the software that is available in RAMP,
- Tools that can be used for collaboration within RAMP,
- Other actions that could be considered for enhancing trust of users in RAMP.

1 Introduction

1.1 Scope and purpose

The purpose of this document is to provide the overview of what approaches RAMP has in place to protect the users and companies in RAMP, especially in regard to their collaboration with other companies within the platform. The document is not concerned with the technical aspects (e.g. technical means for data protection), but is about the processes implemented.

1.2 Relation with work in other Tasks and Work Packages

This document is of Better Factory task T2.4. As such, it is related to the work of other tasks within the same Work Package, but also with other Work Packages of the Better Factory project.

- WP1: Cyber-security aspects, which also play a role in the user trust, take place in this WP, more specifically, the cyber-security of the RAMP IoT platform is addressed (T1.1), the integration of the Digital Twin in RAMP (T1.2) and the cloud infrastructure access (T1.3)
- WP2: T2.1 is concerned about the technical aspect of data protection in RAMP. T2.2 is the collaboration space, which is a part of RAMP that is benefited from enhanced trust, while T2.5 is concerned specifically with the legal aspects.
- WP3 & WP5: Testing of RAMP and feedback and users' concerns on trustworthiness are collected during the matchmaking phase and the Knowledge Transfer Experiments.
- WP4: APPS should also be trustworthy and secure. This is mostly addressed through the work in T1.1.
- WP6 & WP7: Dissemination, but most importantly, business development is supported by ensuring the RAMP trustworthiness.

2 Scope of use protection mechanisms

2.1 Scope of the RAMP protection mechanisms

Protection mechanisms in RAMP aim to ensure the following aspects:

- Confirmation / validation of transactions performed through RAMP
- Enhancement of the credibility of the companies, organisations and software in RAMP
- Protection of transactions taking place within RAMP
- Protection of the data and information shared within RAMP, and especially in the collaboration spaces
- Trust building for the data processing that takes place within RAMP
- Conflict resolution between RAMP companies
- Logging of actions and providing evidence of the occurrence of actions on RAMP

2.2 What is out of the scope of the RAMP protection mechanisms

The following aspects are out of the scope of the RAMP protection mechanisms:

- Any kind of legally-binding mediation in the collaboration or service provision between the organisations in RAMP
- Payments and any other kind of monetary transactions
- User role assignment and credential provisioning, which is the RAMP company's sole responsibility, with the exception of issuing initial user credentials to the user who will set up the RAMP company's account
- Credit worthiness assessment of the companies active on RAMP
- Full use of RAMP on mobile devices
- Verification of accuracy of documents, statements, data and other input uploaded by the RAMP company onto RAMP
- Providing an assessment of, or advice regarding, the legality of RAMP companies' actions, commitments, data or activities on or through RAMP
- Assessing the safety and/or security of the RAMP company's premises, manufacturing line, processes, procedures, products or services
- Assessing the adequacy and compliance of the RAMP company's data governance processes and practices

2.3 Disclaimer of liability

The description of the user protection mechanisms and processes in this document are for information purposes only and shall in no event be construed as a legally binding offering, promise or commitment on the part of the RAMP Consortium Members, nor can it be construed as a legally binding description of the products and services offered by the RAMP Consortium Members through RAMP. The legal relationship between the RAMP Company and the company offering RAMP are solely and exclusively governed by the RAMP Terms and Conditions.

3 Transactions in RAMP

3.1 Scope of service

Trust enhancing in the aspect of transactions, i.e. service provision from a provider to a manufacturing SME, taking place in RAMP is concerned only with those transactions that are made within RAMP. Transactions outside RAMP, i.e. via telephone, email, messaging, etc., cannot be verified by RAMP.

3.2 Previous recommendations

In the previous version of this deliverable, D2.6 [1], the recommended process was based on the usage of the 'Tenders' tool, and the automated verification of a transaction through following up the different tender stages. The recommended process was as follows:

1. A manufacturer launches a tender within RAMP, through the 'Tenders' tool
2. After accepting offers, the manufacturer may accept one or more.
3. When a proposal moves to the 'Contracts' phase in the 'Tenders' tool, the transaction is validated within RAMP. The 'Contracts' phase in 'Tenders' includes a legally-binding contract between the manufacturer and the service supplier, signed on a bilateral basis.

3.3 Action and plan

Based on the feedback from the Better Factory KTEs (first round), the 'Tenders' tool was removed. However, based on the knowledge gained from this process, a new tool targeted to enhance the launching of service requests is in development.[1] The process followed, implements the relevant parts of the above recommendation. A 'Transaction Tracker' tracks the current status of the service request. While the process still depends on a user's input, it does not require a 'manual' transaction claim and confirmation, but tracks the status by watching the user actions.

Action	Transaction Tracker status (after the action)
Manufacturing SME requests a service, describing their use case and potential software solutions from the RAMP Component catalogue.	Searching in RAMP partner network
RAMP administration selects 1 to 5 service providers from the RAMP partner network[2] and recommends them to the Manufacturing SME.	Suggestions received
Manufacturing SME selects one or more service providers for the service provision.	Needs analysis
Service provider makes an initial offer, including the solutions and an estimated price.	Solution refinement
Manufacturing SME and Service provider refine the solution, until the Manufacturing SME accepts the offer.	Contracting
Manufacturing SME and Service provider negotiate the contract, until both sides accept the contract.	Implementation
Service provider implements the service (outside RAMP) and confirms that implementation is completed.	Completed – Unconfirmed
Manufacturing SME confirms the implementation is completed.	Completed - Confirmed

[1] The new service request tool is implemented in the context of another project (KITT4SME), while in the Better Factory the co-creation space was implemented as the 'RAMP Web Workspace'.
[2] The RAMP partner network consists of service providers who have signed a partnership contract with RAMP.

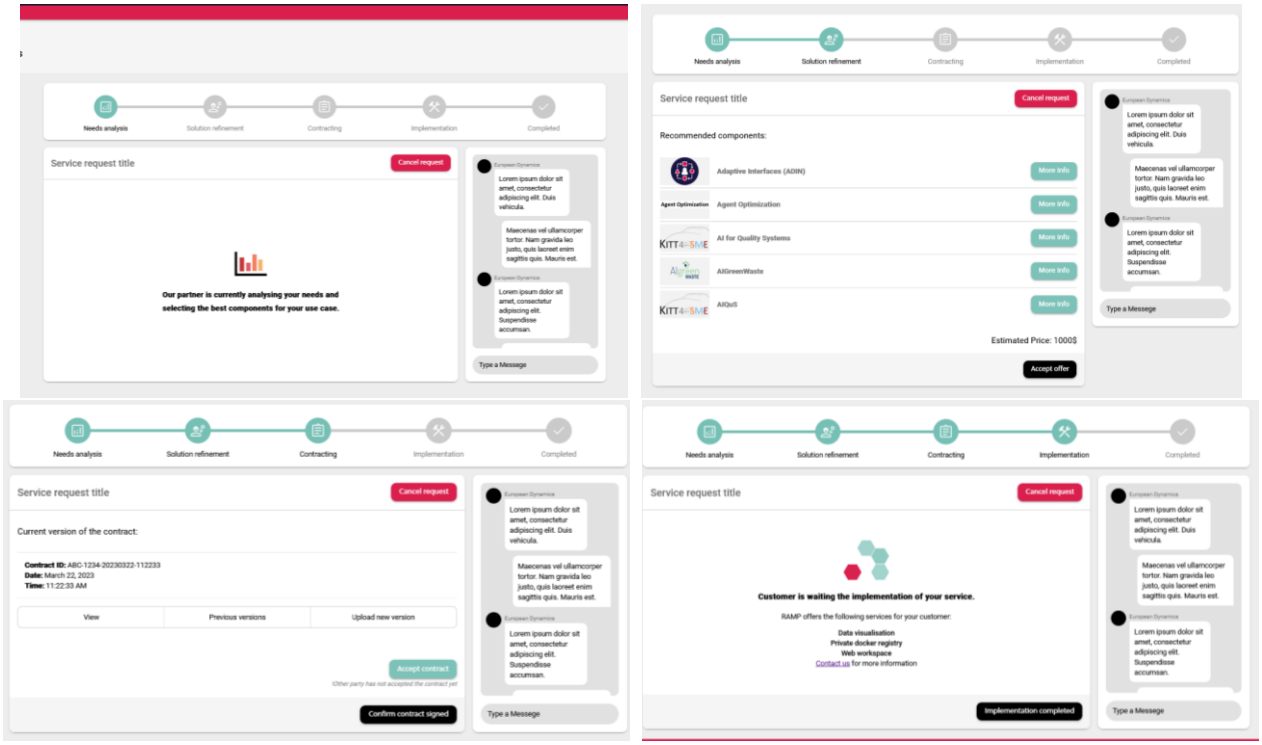

Figure 1: Screenshot of 'Service request' tool that is being developed. Enhancing the transparency for the user, the transaction is tracked as the steps displayed at the top of the screen.

4 Credibility of RAMP companies

Regarding the credibility of companies in RAMP there are three aspects:

- Whether the company is 'officially' signed up in RAMP, and therefore whether its users are authorized to perform negotiations and transactions in RAMP.
- Whether the company is a legit one, and relevant to the RAMP scope. Beyond relevance, ensuring the high quality of the companies, and especially from the suppliers' side is of upmost importance.
- Whether the software components that are available in RAMP are of high quality, to ensure that the components are from trusted vendors and are not highly vulnerable.

4.1 Authorization of companies

4.1.1 Scope

The scope of the authorization mechanism is to verify if an organization profile in RAMP is managed by an authorized person. Previously, it was required that the CEO or a legal representative registers an organization, while it included a waiting time for the RAMP administration team to approve the account. However, this process generated issues in the user experience and uncertainties on the follow up.

4.1.2 Previous recommendations

In the previous version of this deliverable, D2.6 [1], it was recommended to ask the user to submit appropriate documentation upon registration in order to be approved.

4.1.3 Action and plan

Based on the feedback collected, the previous process of waiting for the RAMP administration team to approve a registration caused uncertainties to the users and impacted the user journey. Additionally, for using some features, i.e. other than advertising the organization and its services, it isn't needed to verify an organization or even to be a part of an organization in RAMP. Additionally, users were expecting that their organization profile would be directly visible after adding it to RAMP.

To accommodate the above-mentioned feedback the following features have been implemented:

- A user can sign up to RAMP, directly by self-registration. No RAMP approval is required.
- A system of 'Verified' and 'Unverified' indicators has been implemented in the RAMP catalogue of organisations. Any user can create an organization in the RAMP catalogue. This will be displayed as 'Unverified'. In order to become a 'Verified' organization, RAMP will need to verify the legality and authorization of the person in managing the organization profile in RAMP.

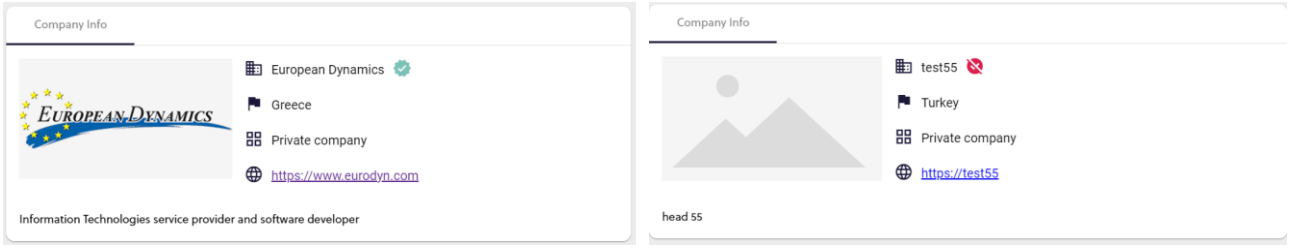

Figure 2: Verified (left) and Unverified (right) organisations. Indicator is displayed next to the organisation name.

The verification process itself is planned to be implemented in the follow up developments. The process will be as follows:

1. User will select the "Verify" organization in their organization's profile edit.
2. User will be asked to upload relevant documentation that may be: Proof of the user being the CEO or legal representative or proof of the person that is CEO or legal representative accompanied by an authorization letter of this person to the user.
3. RAMP administration will review the documentation and will change the organization status to 'Verified' or ask for additional documentation, as needed.

4.2 Quality of RAMP companies

4.2.1 Scope

While the previous process is focused on ensuring that an organization is legit and authorized to be on RAMP, it does not ensure that the organisations in RAMP provide services of high quality. Ensuring the quality of the 3rd-party services in RAMP is another aspect that is reviewed in this paragraph. RAMP should ensure that the services provided by the different actors in the automation value chain are of high quality.

4.2.2 Previous recommendations

On the previous deliverable, D2.6 [1], the following recommendations have been made:

- Include use cases and past customers in the profiles
- Monitor conflicts between organisations and take actions for the potentially problematic ones.
- Perform background check on the quality of the companies that register.

4.2.3 Action and plan

The inclusion of use cases and past customers is planned to be implemented in the next 6 months. This will include a) use cases from verified transactions, as described in the previous chapter, and b) use cases that the organization add themselves.

The monitoring of conflicts is a continuous administrative process.

The background check is slightly modified as follows. Since it is not scalable to perform a background check on all the organizations signing up on RAMP, this is now substituted by the 'RAMP Partner Network'. This network consists of service providers with whom RAMP will sign a partnership agreement, and as such will be able to both perform a background check, but also to ensure the quality of their services through RAMP in the future. A separate section in RAMP will show only these partners, while they will be also shown with a visual indicator 'RAMP partner' in the organizations catalogue.

Additionally, while a star-system was proved not usable and was not adopted, a 'recommendation' system, which would allow users to post comments on organisations could be implemented.

4.3 Quality of software components

4.3.1 Scope

RAMP provides access, either direct with downloads or indirect, to software components. Ensuring the quality of these components is also important for users' trust in RAMP.

4.3.2 Previous recommendations

This had not been previously considered.

4.3.3 Action and plan

The actions in RAMP for trust enhancing are implemented in 2 aspect:

- One aspect is to indicate to the user the components that come from verified and from RAMP partners. This way, while browsing the components catalogue, it is easy to quickly review and filter software components in 3 levels of quality:
    - Components coming from 'Unverified' organizations
    - Components coming from 'Verified' organizations
    - Components coming from 'RAMP partners'
- Second aspect is to perform a vulnerability scan on all components that are uploaded to the RAMP docker registry. The scan is automatically performed when the image is uploaded, while the detailed results are displayed to the user, but also to the developer with appropriate corrective actions.

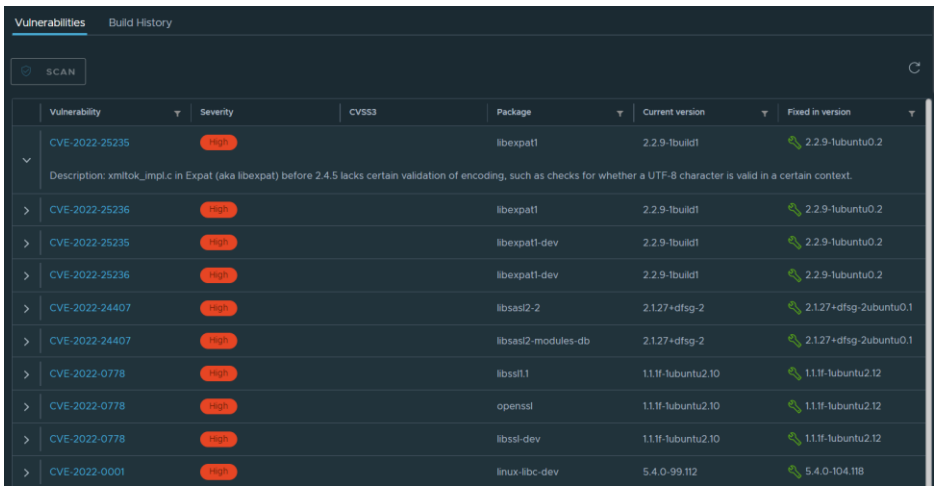

Figure 3: RAMP docker registry vulnerability scan, with vulnerability details, references and corrective actions.

5 Online collaboration and data protection

RAMP provides a number of tools that allow online collaboration between organisations, for example between a manufacturer and an automation technology provider, etc. These tools provide functionalities where documentation and media may be shared. This data in may include sensitive information, trade secrets. For example, during a service provision for automation, details and diagrams from the factory could be shared between the manufacturer and the provider, or details about the technologies of the provider that give them competitive advantage, etc. While from the RAMP side this data is protected, from organizational and technical point of view, it is important to also increase the awareness and enhance the trust of the organisations in RAMP, so they can not only 'be', but also 'feel' safe in using these tools and sharing this data through RAMP.

The related tools for collaboration where such data is shared include:

- Web Workspace, a tool where different users may collaboratively use applications,
- Factory Dashboard, a tool that allows the visualization of data from the factory floor (sensors, equipment, etc.),
- Digital Twin, a tool in 'Automation' projects, which allows the 3D visualization and simulation of the factory floor, a production line or a work cell,
- Service request tool, which enable a service and contract negotiation between a Manufacturing SME and a Service Provider.

The protection of this data is ensured through the work in Task T2.1.

RAMP should clearly communicate the terms and conditions of using the platform, as well as of the data protection measures, to users. This includes outlining the responsibilities of manufacturers and service providers, the process for resolving disputes, and any fees or commissions that RAMP may charge. While the text itself has been prepared, it should be more visible in relevant places within the platform according to user actions.

6 More considerations on trust enhancement

Based on literature research [2] [3] [4] [5] [6] [7] [8] [9] [10] [11], the following actions are important in enhancing trust of users in RAMP:

Recommendation	Current status
Be transparent: RAMP should provide clear and concise information about how the platform works, what data is collected, and how it is used. This can be done through the development of a privacy policy, terms and conditions, and user agreements that are easy to understand and accessible to all users.	While RAMP includes terms and conditions for users in the form of downloadable file, a simpler version should be also made available online. This should also give information on the cybersecurity measures used to protect user data.
Establish a secure data environment: RAMP should ensure that data is collected, processed, and stored securely. This can be achieved through the implementation of strong security measures such as encryption, firewalls, and regular vulnerability assessments. Additionally, RAMP should comply with data protection regulations such as GDPR.	This is implemented and ensured, also by relevant certifications for European Dynamics that hosts the RAMP platform. (ISO-27001 and ISO-9001 certifications)
Provide user support: RAMP should have a responsive support team that is available to help users with any issues they encounter. This can include technical support, training, and guidance on how to use the platform effectively.	While there is a contact form to provide user support, a friendlier user interface on the status of the requests could be implemented.
Foster a community of trust: RAMP should actively work to build a community of users who trust the platform. This can be achieved through regular communication, sharing success stories, and fostering a sense of collaboration among users.	RAMP does not implement this action as of yet. Success stories, especially from the KTEs, could be better advertised.
Ensure service quality: RAMP should work with its service providers to ensure that the services offered are of high quality. This can be achieved through the establishment of clear service level agreements (SLAs) and regular monitoring of service performance.	This is already in progress, in the form of the RAMP partner network.
Promote user feedback: RAMP should actively seek user feedback to improve the platform. This can be done through surveys, user forums, and other feedback mechanisms. User feedback can be used to identify areas for improvement and to demonstrate a commitment to continuous improvement.	Currently RAMP does not include frequent feedback calls while the user is browsing. It could be considered, but should be carefully designed so that it does not disrupt the user journey.
Provide clear pricing: RAMP should be transparent about the pricing of its services. This can be achieved through the development of clear pricing models that are easy to understand and accessible to all users.	This is already in progress, in the RAMP business model development.

Recommendation	Current status
Leverage social proof: RAMP should use social proof to demonstrate the trustworthiness of the platform. This can include sharing user testimonials, case studies, and other success stories. Additionally, RAMP can leverage social proof by partnering with reputable organizations and displaying trust badges on the platform.	While trust badges are already included in the form of the RAMP partner network, better advertising could be considered (as above).
Conduct regular security audits: RAMP should conduct regular security audits to ensure that the platform remains secure and up-to-date. This can be done by partnering with reputable security firms that specialize in conducting audits and providing recommendations for improvement.	Security, vulnerability and ISO audits are already performed regularly.
Establish a reputation system: RAMP should consider implementing a reputation system that allows users to rate and review service providers. This can help to build trust among users and incentivize service providers to maintain high standards of service quality.	Action plan already included in previous chapter.
Provide clear communication: RAMP should communicate clearly and frequently with its users, particularly when it comes to any changes to the platform or service offerings. This can be done through newsletters, email updates, and other communication channels.	Currently RAMP does not post publicly the updates on the platform. This could be considered for implementation.
Publish regular reports: RAMP should publish regular reports that provide insights into the performance of the platform and its service providers. This can include metrics such as uptime, service response times, and customer satisfaction scores.	Currently such data, although available, is not utilized to generate such reports. This could be considered for implementation.
Collaborate with trusted partners: RAMP should partner with reputable organizations that are known for their expertise in the automation value chain. This can help to build trust among users and provide them with confidence in the quality of services provided through the platform.	Already in progress in the form of the RAMP partner network.
Offer guarantees: RAMP could consider offering guarantees to its users, such as a money-back guarantee or a satisfaction guarantee. This can help to build trust and incentivize service providers to maintain high standards of service quality.	This is a business aspect that should be considered in the business model development. Such guarantees, when related to the RAMP partner network, could be considered.
Provide multiple communication channels: RAMP should provide multiple communication channels for its users, such as email, phone, and chat support. This can help to ensure that users can get help quickly and easily when they need it.	Currently, only email support is provided, as there are not enough resources as of yet to provide live telephone or chat support. This should be considered in the exploitation phase of RAMP.

Recommendation	Current status
Engage with users on social media: RAMP should engage with its users on social media platforms such as LinkedIn and Twitter. This can help to build a sense of community among users and provide a platform for sharing success stories and other positive feedback.	Currently, RAMP is promoted through the participating projects' social media. Individual RAMP social profiles could be considered in the exploitation phase.
Offer dispute resolution: RAMP should have a clear process for dispute resolution in case of issues between service providers and manufacturing SMEs. This can help to build trust by showing that RAMP takes user concerns seriously and is committed to resolving issues in a fair and timely manner.	This is already planned, and detailed in the previous version of this deliverable, D2.6 [1].
Offer a trial period: RAMP could consider offering a trial period for new users to try out the platform and its services before committing to a long-term engagement. This can help to build trust by giving users the opportunity to evaluate the platform and service providers before making a commitment.	A trial period is already considered in the business model design.

7 Conclusions

To sum up, the following actions are recommended for the RAMP short- and long-term future, along with their current status:

In progress:

- Transaction tracking in service requests.
- Establishment and agreements/contracts for the RAMP partner network.

Planned:

- Implementation of organization verification process, with documentation upload.
- Use cases in organization profiles.
- Clear communication on terms and conditions, as well as data protection measures.
- Better advertisement and marketing of the RAMP use cases.

Considered:

- Recommendation system for organizations.
- Friendlier user interface for user feedback status tracking.
- Ask for frequent user feedback.
- Publish updates on the platform changes.
- Publish performance reports.

To be considered during exploitation:

- Provide guarantees, for service provision through the RAMP partner network.
- Live (chat, telephone) user support.
- Individual social media profiles.
- Trial period.

8 References

[1] P. Bouklis, "D2.6 User protection processes and mechanisms," Better Factory (Grant agreement No. 951813), Athens, Greece, 2021.

[2] N. Albinson, S. Balaji and Y. Chu, "Building digital trust: Technology can lead the way," Deloitte, 2019.

[3] J. Boehm, L. Grennan, A. Singla and K. Smaje, "Why digital trust trully matters," McKinsey & Company, 2022.

[4] Gartner, "How Service Leaders Can Increase Customer Loyalty".

[5] KPMG P/S, "Build trust through cybersecurity and privacy," 2022.

[6] J. Nielsen, "Trust or Bust: Communicating Trustworthiness in Web Design," Nielsen Norman Group, 1999.

[7] "Regulation (EU) 2016/679 of the European Parliament and of the Council," *Official Journal of the European Union,* 2016.

[8] N. Resnick, "The Psychology of Social Proof (and Why You Need Your Customers' Help)," HubSpot, 2022.

[9] State of California Department of Justice, "California Consumer Privacy Act (CCPA)," 2018.

[10] S. Wells, "How To Build Trust With Your Customers," Forbes, 2019.

[11] P. Zak, "The Neuroscience of Trust," Harvard Business Publishing, 2017.

INESCTEC 35 SUPSI aimen TECHNOLOGY CENTRE Cyprus University of Technology Fraunhofer

FundingBox NCRI INOVA+ GLUON waag technology & society

European Dynamics TIMELEX MOBILE WORLD CAPITAL BARCELONA Hermia Yrityskehitys Oy HOLONIX BRING THINGS TO LIFE

TOP data science A MORPHO COMPANY industrial generation network GESTALT ROBOTICS In4Art guiding curiosity.... OULUN YLIOPISTO

CLUSTER MOBILIER TRANSILVAN TECOS Razvojni center orodjarstva Slovenije ICT cluster LATVIJAS PĀRTIKAS UZŅĒMUMU FEDERĀCIJA BYDGOSZCZ INDUSTRIAL CLUSTER

clutex klastr technické textilie PÉCS-BARANYAI KERESKEDELMI ÉS IPARKAMARA alapítva 1881

H2020 Innovation Action – This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 951813.