
Community.OS - Mosa Data Processing & Organisation Privacy Terms

Document	Mosa Data Processing & Organisation Privacy Terms
Document Version	v1.0
Reviewed	27th September 2026
Status	Approved
Parent Company	Sidekick Platforms
Platform Brand	Community.OS
Consumer Product	Mosa
Brand Promise	Making Participation Visible
Core Message	When participation becomes visible, communities become stronger.
Supporting Line	Every little bit helps.
Guide	Pitch

Table of Contents

Community.OS - Mosa Data Processing & Organisation Privacy Terms	1
Table of Contents	2
1. About These Terms	3
2. Core Privacy Principle	4
3. Information Categories and Responsibility	5
4. Organisation Collection and Use	6
5. Organisation Responsibilities	7
6. Sidekick Platforms Responsibilities	8
7. Joint and Distinct Responsibilities	8
8. Children and Young People	9
9. Sensitive Information	10
10. Health, Safety and Safeguarding Information	10
11. Organisation Assertions and Accuracy	11
12. Access and Correction	11
13. Communication Data	12
14. Exports	12
15. Organisation-Controlled Integrations	13
16. Information Already Transferred to Organisation Systems	14
17. Sidekick Platforms Service Providers	14
18. Subprocessors	15
19. Overseas Processing and Disclosure	16
20. Security	16
21. Privacy and Security Incidents	17
22. Notifiable Data Breaches	18
23. Privacy Complaints	18
24. Retention	18
25. Deletion and De-Identification	19
26. Organisation Exit	19
27. Organisation Data Requests on Exit	20
28. Auditability and Records	20
29. Assurance and Information Requests	21
30. Audits by the Organisation	22
31. Government, Regulatory and Legal Requests	22
32. Confidentiality	23
33. Changes to These Terms	23
34. Order of Precedence	23
35. Liability and Responsibility	24
36. Contact	24
37. Definitions	25
Data Processing & Organisation Privacy Commitment	26

1. About These Terms

1.1 Purpose

These Data Processing & Organisation Privacy Terms explain how privacy and personal information responsibilities are allocated between:

OSA Management Pty Ltd (ABN 62 677 945 863), trading as Sidekick Platforms

and:

an Organisation using Community.OS or Mosa.

These Terms supplement the **Mosa Organisation Terms**.

They are intended to provide greater clarity about:

- Organisation-provided information;
- participant-controlled information;
- Organisation access;
- collection and use;
- sensitive information;
- children and young people;
- integrations;
- exports;
- service providers;
- overseas processing;
- security;
- privacy incidents;
- access and correction;
- retention;
- deletion;
- and Organisation exit.

1.2 Relationship With Other Documents

These Terms should be read together with:

- the Mosa Organisation Terms;
- the Mosa Privacy Policy;
- Privacy at Mosa;
- the Children & Young People Privacy Notice;
- applicable Organisation privacy notices;
- any applicable Order Form;
- Community Space terms;
- Enterprise terms;
- and other expressly incorporated privacy or data-processing schedules.

1.3 These Terms Do Not Create a Universal Controller / Processor Model

Privacy responsibilities within Community.OS depend on the actual information and activity involved.

Different circumstances may involve:

- Sidekick Platforms determining the relevant purpose;
- the Organisation determining the relevant purpose;
- each party determining separate purposes;
- both parties having responsibilities concerning the same information;
- or one party acting primarily to provide a capability requested by the other.

The parties should therefore not assume that one universal privacy role applies to all Community.OS information.

Australian privacy law generally regulates APP entities according to the personal information they hold and the acts or practices they undertake, rather than applying the GDPR controller / processor distinction as the universal Australian model. [OAIC](#)

2. Core Privacy Principle

2.1 Responsibility Follows Purpose, Authority and Control

The parties intend privacy responsibility to follow:

- who collected the information;
- where it came from;
- who determines the relevant purpose;
- who controls the relevant capability;
- who can access or disclose it;
- the relationship with the Person;
- and applicable law.

2.2 The Organisation Does Not Own the Person

The Organisation may have legitimate records and responsibilities relating to a Person.

It does not own:

- the Person's Mosa identity;
- unrelated Organisation relationships;
- unrelated Community Story;
- unrelated Household relationships;
- private communications outside its legitimate context;
- or other information merely because Community.OS can associate that information with the same Person.

The canonical Privacy Architecture expressly establishes that Organisation relationships create context, not universal access. c.OS - Security, Reliability & ...

2.3 Technical Access Does Not Create Privacy Authority

The fact that Community.OS can technically display, transfer, export or integrate information does not itself create a legitimate right to use that information.

3. Information Categories and Responsibility

3.1 Participant-Controlled Information

Some information is primarily managed as part of the Person's persistent Mosa identity.

This may include information such as:

- participant-controlled profile information;
- preferred name;
- Handle;
- profile image;
- communication preferences;
- selected Community Story presentation;
- and other participant-managed information.

An Organisation may receive access to relevant parts of that information where its legitimate relationship and authority justify it.

3.2 Organisation-Provided Information

An Organisation may provide information concerning a Person.

Examples may include:

- membership status;
- Organisation-specific identifiers;
- roles;
- attendance;
- participation records;
- Organisation invitations;
- Organisation-specific eligibility;
- Organisation assertions;
- and other legitimate Organisation records.

Where appropriate, Community.OS may preserve the Organisation as the source of that information.

3.3 Verified Information

Some information may be independently verified.

Examples may include:

- qualifications;
- checks;

- certifications;
- or other trusted attributes.

Community.OS may distinguish the verified outcome from the underlying evidence.

3.4 Derived Information

Community.OS may derive information according to defined platform rules.

Examples may include:

- eligibility outcomes;
- requirement status;
- participation calculations;
- Community Credits;
- or other system-derived states.

3.5 Historical Records

An Organisation may legitimately steward historical records relating to its own relationship with a Person.

Historical stewardship does not necessarily create continuing access to that Person's current profile or unrelated information.

4. Organisation Collection and Use

4.1 Legitimate Purpose Required

The Organisation must only request, collect, access, use or disclose personal information where it has a legitimate reason to do so and where the activity is permitted by applicable law.

4.2 Minimum Necessary Information

The Organisation should not request information merely because Community.OS makes it technically possible.

Information should be reasonably necessary for purposes such as:

- membership;
- participation;
- communication;
- safety;
- safeguarding;
- qualification requirements;
- payments;
- governance;
- compliance;
- or another legitimate Organisation purpose.

4.3 Trusted Outcome Over Unnecessary Evidence

Where Community.OS can allow the Organisation to perform the legitimate task without exposing unnecessary underlying information, the Organisation should ordinarily use that capability.

For example:

Qualification requirement satisfied

may be sufficient where the Organisation does not genuinely need the underlying document.

The canonical Privacy Architecture expressly prefers capability over unnecessary disclosure. c.OS - Privacy, Consent & Safeg...

4.4 Information Should Reveal Itself When Needed

The intended model is:

Information becomes available when the legitimate relationship, purpose and authority require it.

not:

Collect everything now in case it becomes useful later.

5. Organisation Responsibilities

5.1 Compliance With Applicable Law

The Organisation is responsible for complying with privacy and information-handling requirements that apply to it.

5.2 Appropriate Notices

Where the Organisation independently collects personal information or determines its own purposes, it is responsible for providing any privacy notice or other information required by law.

5.3 Appropriate Authority

The Organisation must ensure that people accessing participant information through Community.OS have appropriate Organisation authority.

5.4 Periodic Access Review

The Organisation must take reasonable steps to periodically review:

- administrators;
- managers;
- roles;

- significant permissions;
- export access;
- integration access;
- and other consequential information access.

Access that is no longer reasonably required should be reduced or removed.

5.5 Protecting Information Under Organisation Control

The Organisation is responsible for appropriately protecting information once it enters systems or environments controlled by the Organisation.

6. Sidekick Platforms Responsibilities

6.1 Community.OS Privacy Architecture

We are responsible for designing and operating Community.OS so that platform access is constrained according to legitimate identity, relationship, purpose, authority, privacy and safeguarding rules.

6.2 Platform Access Controls

We are responsible for access-control mechanisms we operate within Community.OS.

6.3 Internal Access

Sidekick Platforms personnel do not receive unrestricted participant information access merely because they work for us.

Internal access should remain:

- purposeful;
- appropriately scoped;
- attributable;
- revocable;
- and proportionate to operational need.

6.4 Service Providers

We are responsible for selecting and governing service providers we use to operate Community.OS according to our applicable legal and contractual obligations.

7. Joint and Distinct Responsibilities

7.1 Both Parties May Have Responsibilities

There may be circumstances where both Sidekick Platforms and the Organisation have privacy obligations concerning the same Person or information.

That does not necessarily mean the obligations are identical.

7.2 Independent Purposes

Where a party independently determines a legitimate purpose for handling information, that party remains responsible for that purpose.

7.3 One Party's Compliance Does Not Automatically Satisfy the Other's

An Organisation should not assume that Sidekick Platforms' Privacy Policy satisfies every privacy obligation of the Organisation.

Likewise, an Organisation's privacy notice does not replace our own privacy obligations.

8. Children and Young People

8.1 Additional Care

Information involving children and young people may require additional privacy and safeguarding consideration.

8.2 Representation

Where a parent, guardian or other representative acts for a young Person, the Organisation must not assume authority solely because a relationship appears within Community.OS.

Relevant authority depends on the relationship and context.

8.3 Organisation Responsibilities

Where an Organisation works with children or young people, it remains responsible for applicable:

- child safety;
- safeguarding;
- privacy;
- communication;
- screening;
- and other legal requirements.

8.4 Minimum Necessary Access

Information about young people should not become broadly visible merely because multiple Organisation users have administrative roles.

9. Sensitive Information

9.1 Additional Protection

Sensitive information requires additional care.

This may include:

- Health & Safety Information;
- certain qualification or screening information;
- safeguarding information;
- or other sensitive information recognised under applicable law.

9.2 Organisation Access

An Organisation should restrict sensitive information to people with legitimate need and authority.

9.3 Underlying Evidence

Where an Organisation only requires an outcome, it should not demand underlying sensitive evidence without a legitimate reason.

9.4 Sidekick Platforms Controls

Community.OS may apply stronger:

- access controls;
- auditability;
- visibility restrictions;
- consent requirements;
- or other protections

to sensitive information.

10. Health, Safety and Safeguarding Information

10.1 Legitimate Operational Need

An Organisation may legitimately require certain health, safety or safeguarding information to support participation.

10.2 Purpose Limitation

That information should not be repurposed for unrelated Organisation activity merely because it is accessible.

10.3 Limited Visibility

Access should be limited according to:

- role;
- activity;
- relationship;
- need;
- and safeguarding requirements.

11. Organisation Assertions and Accuracy

11.1 Organisation Assertions

Where an Organisation provides information concerning a Person, Community.OS may identify that information as Organisation-sourced.

11.2 Accuracy Responsibility

The Organisation must take reasonable steps to ensure information it provides is accurate, current and appropriate for the purpose for which it is supplied.

11.3 Disputed Information

Where information is disputed, Community.OS may preserve:

- its original source;
- the disputed state;
- correction history;
- or other provenance

instead of silently overwriting a legitimate historical record.

12. Access and Correction

12.1 Participant Requests

A participant may seek access to or correction of personal information concerning them.

12.2 Sidekick Platforms Information

Where the information is held or controlled within our privacy responsibility, we will handle applicable access or correction requests according to law and our Privacy Policy.

12.3 Organisation Information

Where a request concerns information maintained by the Organisation for its own purposes, the Organisation may need to respond.

12.4 Cooperation

The parties should reasonably cooperate where an access or correction request involves both platform-managed and Organisation-managed information.

13. Communication Data

13.1 Operational Communications

An Organisation may use Community.OS communications for legitimate Organisation purposes.

13.2 Communication Authority

The Organisation must only use communication capabilities consistent with:

- the relevant relationship;
- applicable law;
- privacy;
- safeguarding;
- and applicable communication rules.

13.3 Private and Organisation Communications Are Different

Organisation-controlled communications and participant-controlled personal conversations may have different information access and retention rules.

14. Exports

14.1 Export Must Follow Existing Authority

An Organisation may only export information it is legitimately entitled to access.

Export functionality must not create broader information authority than the Organisation has within Community.OS.

14.2 Purpose Before Export

Before exporting information, the Organisation should consider whether the legitimate purpose can instead be achieved through:

- an in-platform capability;
- a trusted integration;

-
- a purpose-specific report;
 - or another lower-risk method.

The Privacy Architecture explicitly prefers in-platform capability and scoped integrations before broad raw-data export where practical. c.OS - Privacy, Consent & Safeg...

14.3 Responsibility After Export

Once personal information is legitimately exported into an Organisation-controlled environment, the Organisation becomes responsible for that copy.

This includes responsibility for:

- access;
- use;
- storage;
- security;
- retention;
- further disclosure;
- deletion;
- and any later transfer.

14.4 Export Does Not Transfer Ownership of the Person

Exporting information does not give the Organisation ownership of:

- the Person;
- their Mosa identity;
- unrelated Community Story;
- or information outside the Organisation's legitimate authority.

15. Organisation-Controlled Integrations

15.1 Organisation Selection

Where the Organisation selects or controls an external system, the Organisation is responsible for assessing whether that system is appropriate for the Organisation's intended use.

15.2 Integration Authority

An external system connected by the Organisation must not receive broader access than the Organisation is legitimately entitled to provide.

15.3 API Access Is Not Super-Admin Access

Programmatic access does not create additional privacy authority.

An API credential must not become a shortcut around Community.OS access controls.

The canonical architecture expressly requires API authority to remain within the same underlying privacy boundaries as ordinary platform access. c.OS - Privacy, Consent & Safeg...

15.4 Read and Write Permissions

Permission to read information does not automatically include permission to:

- create;
- update;
- delete;
- or trigger unrelated actions.

15.5 Revocation

Where supported, the Organisation should disconnect integrations that are no longer required.

Revocation should end future authorised access.

16. Information Already Transferred to Organisation Systems

16.1 Revocation Does Not Automatically Delete Existing Copies

Disconnecting an integration or ending Community.OS access does not necessarily remove information already legitimately transferred into an Organisation-controlled system.

16.2 Organisation Responsibility Continues

The Organisation remains responsible for those copies according to its applicable legal, privacy and retention obligations.

This follows the canonical Privacy Architecture, which expressly recognises that revocation can end future access without causing previously transferred information to disappear automatically. c.OS - Privacy, Consent & Safeg...

17. Sidekick Platforms Service Providers

17.1 Use of Specialist Providers

We may use specialist providers for services such as:

- cloud infrastructure;
- database and storage;
- authentication;
- email;
- notifications;
- payment processing;
- monitoring;
- analytics;

-
- security;
 - customer support;
 - qualification verification;
 - communications infrastructure;
 - and other Community.OS services.

17.2 Minimum Necessary Provider Access

We seek to provide service providers only the information and capability reasonably required to perform their defined service.

17.3 Provider Use Is Limited

A provider processing information for Community.OS does not thereby receive independent authority to use participant information for unrelated purposes.

17.4 Risk-Based Provider Review

We may apply different levels of provider assurance depending on:

- information sensitivity;
- access;
- service criticality;
- privacy risk;
- security risk;
- and operational consequence.

The canonical Privacy Architecture expressly requires greater scrutiny for providers handling children's information, health information, identity evidence, communications, safeguarding information or large-scale participant data. c.OS - Privacy at Mosa - v1.0.2...

18. Subprocessors

18.1 Subprocessor Use

A service provider may itself rely on subprocessors.

18.2 Governance

For consequential services, we should understand material subprocessor relationships where reasonably available.

18.3 Transparency

We may maintain and progressively publish information about material service providers and subprocessors where appropriate.

18.4 Provider Changes

We may change providers or subprocessors as Community.OS evolves, provided that doing so remains consistent with applicable privacy, security and contractual obligations.

19. Overseas Processing and Disclosure

19.1 Overseas Services May Be Used

Some providers, infrastructure or recipients may be located outside Australia.

19.2 Australian Privacy Obligations

Where Australian privacy law applies to a cross-border disclosure, the relevant party must comply with its obligations.

APP 8 generally requires an APP entity to take reasonable steps before disclosing personal information to an overseas recipient to ensure the recipient does not breach the APPs, subject to specific exceptions. In certain circumstances the Australian entity may also be accountable for the overseas recipient's conduct. [OAIC](#)

19.3 Sidekick Platforms Providers

Where we select and control an overseas provider, we are responsible for our applicable cross-border privacy obligations.

19.4 Organisation-Controlled Overseas Systems

Where the Organisation chooses to transfer information to or connect an overseas external system under its control, the Organisation is responsible for its applicable cross-border obligations concerning that disclosure.

19.5 No Assumed Consent

The parties should not assume that general acceptance of these Terms constitutes consent to every overseas disclosure where applicable law requires a more specific interaction.

20. Security

20.1 Shared Security Responsibility

Security responsibility follows meaningful control.

20.2 Sidekick Platforms Controls

We are responsible for security controls within Community.OS that we operate.

20.3 Organisation Controls

The Organisation is responsible for areas it controls, including:

- administrator selection;
- administrator access review;
- Organisation-controlled devices;
- Organisation-controlled systems;
- exported information;
- integration credentials it controls;
- and information held outside Community.OS.

20.4 Minimum Necessary Access

Both parties should seek to restrict information access to people and systems that reasonably need it.

21. Privacy and Security Incidents

21.1 Incident Cooperation

Where a privacy or security incident may involve both Community.OS and the Organisation, the parties should reasonably cooperate.

21.2 Notification Between the Parties

A party becoming aware of a material incident affecting information within the other party's responsibility should notify the other party where reasonably necessary to support investigation, containment or legal compliance.

21.3 Legal Notification

Each party remains responsible for determining and meeting any breach-notification obligation that applies to it.

21.4 Information Sharing During an Incident

Incident information should be shared to the extent reasonably necessary to:

- investigate;
- contain;
- remediate;
- assess notification obligations;
- protect affected people;
- and comply with law.

22. Notifiable Data Breaches

22.1 Australian NDB Scheme

Where the Australian Notifiable Data Breaches scheme applies, the party with the relevant statutory obligation remains responsible for meeting that obligation.

22.2 Cooperation

Where responsibility overlaps or facts are held by both parties, the parties should cooperate reasonably so the relevant assessment and notification can occur.

23. Privacy Complaints

23.1 Complaints About Sidekick Platforms

Complaints concerning our handling of personal information should be directed to us.

23.2 Complaints About the Organisation

Complaints concerning an Organisation's independent handling of personal information may need to be handled by the Organisation.

23.3 Mixed Complaints

Where a complaint involves both parties, they should cooperate sufficiently to determine:

- what occurred;
- which information was involved;
- which party controlled the relevant conduct;
- and the appropriate response.

24. Retention

24.1 Retention Depends on Purpose

Neither party should retain personal information indefinitely merely because it once had a legitimate reason to hold it.

24.2 Organisation Retention

The Organisation is responsible for retention obligations applying to Organisation-controlled copies and records.

24.3 Community.OS Retention

We are responsible for retention decisions concerning information held within Community.OS according to:

- our Privacy Policy;
- legitimate platform purposes;
- applicable law;
- safeguarding;
- historical integrity;
- security;
- and relevant contractual obligations.

25. Deletion and De-Identification

25.1 Different Records May Have Different Outcomes

Deletion of one category of information does not necessarily require deletion of every record relating to the Person.

25.2 Historical Records

Legitimate historical Organisation records may remain where appropriate.

25.3 Participant Identity

The Organisation's departure or deletion request does not give it authority to delete a Person's broader Mosa identity merely because that Person had an Organisation relationship.

25.4 De-Identification

Where identifiable information is no longer required, de-identification may be appropriate where permitted by law and technically meaningful.

26. Organisation Exit

26.1 Ending the Organisation Relationship

When the Organisation leaves Community.OS, its future information access should end or reduce according to the ended relationship.

26.2 Organisation Export

Where an applicable paid plan includes export functionality, the Organisation should export legitimate Organisation information it requires before that subscription ends.

26.3 Export Scope

The Organisation's entitlement is limited to information it legitimately stewards or is authorised to receive.

It does not extend to everything Community.OS happens to know about its participants.

The canonical Privacy Architecture expressly makes this distinction for Organisation exit and migration. c.OS - Privacy, Consent & Safeg...

26.4 Participant Continuity

Participants may retain their:

- Mosa identity;
- Community Story;
- unrelated Organisation relationships;
- and other legitimate platform information

after the Organisation leaves.

27. Organisation Data Requests on Exit

27.1 No Automatic Continuing Platform Access

Ending a subscription does not create continuing access to paid Organisation functionality.

27.2 Legal Rights Remain

Nothing prevents the Organisation from exercising any information-access or portability right that applicable law or another binding agreement requires.

28. Auditability and Records

28.1 Consequential Actions

Community.OS may retain records of significant privacy and information actions such as:

- administrator changes;
- exports;
- integrations;
- agreements;
- permission changes;
- sensitive information access;
- or other consequential activity.

28.2 Purpose

Audit records may support:

- security;
- privacy;
- safeguarding;

- dispute resolution;
- incident investigation;
- and legal obligations.

28.3 Proportionate Auditability

Auditability does not justify unnecessary surveillance.

29. Assurance and Information Requests

29.1 Reasonable Customer Assurance

We may provide reasonable information about our privacy, security and supplier practices to support Organisation assurance.

29.2 Scope

The level of information may depend on:

- customer size;
- plan;
- risk;
- procurement requirements;
- confidentiality;
- and available assurance material.

29.3 Restricted Material

We are not required to provide information where disclosure would itself create unreasonable:

- security;
- confidentiality;
- privacy;
- contractual;
- or supplier risk.

29.4 Independent Assurance

As Community.OS matures, we may develop additional:

- audit;
- certification;
- penetration testing;
- security assessment;
- or other assurance mechanisms.

30. Audits by the Organisation

30.1 No Unrestricted Audit Right

These Terms do not give every Organisation an unrestricted right to inspect our systems, source code, infrastructure or other customers' information.

30.2 Reasonable Alternative Assurance

Where an Organisation reasonably requires assurance, we may satisfy that requirement through appropriate:

- documentation;
- certifications;
- summaries;
- questionnaires;
- independent reports;
- controlled evidence;
- or other proportionate methods.

30.3 Enterprise Arrangements

More detailed audit or assurance rights may be agreed for Enterprise arrangements where appropriate.

31. Government, Regulatory and Legal Requests

31.1 Lawful Requests

Either party may be required to respond to:

- court orders;
- subpoenas;
- regulatory requests;
- law enforcement requests;
- or other lawful information demands.

31.2 Responsibility

The party receiving the request is responsible for determining its obligations.

31.3 Cooperation

Where a lawful request requires cooperation from the other party, reasonable assistance may be provided where legally permitted.

32. Confidentiality

32.1 Privacy and Confidentiality Are Different

Personal information may also be confidential, but privacy obligations are not replaced by general contractual confidentiality obligations.

32.2 Confidential Handling

Both parties should protect confidential information according to:

- applicable law;
- the Organisation Terms;
- and any other applicable contractual obligations.

33. Changes to These Terms

33.1 Updates

We may update these Terms as:

- law changes;
- Community.OS changes;
- provider arrangements change;
- international operations evolve;
- privacy architecture evolves;
- or new Community Spaces require different treatment.

33.2 Material Changes

Where a material change affects the Organisation's obligations or our contractual privacy commitments, we will provide appropriate notice.

33.3 Reacceptance

Where required, an authorised Organisation representative may need to accept an updated version.

33.4 Historical Versions

A new version does not rewrite the privacy responsibilities that applied to earlier activity.

34. Order of Precedence

Where these Terms conflict with the Mosa Organisation Terms concerning privacy and data-processing responsibilities, these Terms should prevail to the extent of the privacy-specific inconsistency unless a more specific signed agreement expressly states otherwise.

Mandatory legal requirements always prevail.

35. Liability and Responsibility

35.1 Organisation-Controlled Information

The Organisation remains responsible for privacy failures arising from information or systems properly within its control, subject to applicable law and the Organisation Terms.

35.2 Sidekick Platforms-Controlled Information

We remain responsible for privacy failures arising from Community.OS systems or conduct properly within our control, subject to applicable law and the Organisation Terms.

35.3 No Transfer Through Connectivity

The use of Community.OS to connect the parties does not automatically transfer one party's privacy responsibility to the other.

35.4 Organisation Terms Apply

Applicable liability limitations, indemnities and mandatory rights in the Mosa Organisation Terms also apply to these Terms.

36. Contact

Community.OS and Mosa are operated by:

OSA Management Pty Ltd
ABN 62 677 945 863
Trading as Sidekick Platforms

Privacy and Organisation enquiries:

hello@oncommunityos.com

37. Definitions

37.1 Community.OS

Community.OS means the community operating platform developed and operated by OSA Management Pty Ltd.

37.2 Mosa

Mosa means the participant-facing experience built on Community.OS.

37.3 Organisation

Organisation means the organisation entering these Terms.

37.4 Organisation-Controlled System

Organisation-Controlled System means an external system, provider, application or environment selected or controlled by the Organisation rather than by Sidekick Platforms.

37.5 Organisation-Provided Information

Organisation-Provided Information means information supplied, asserted, created or maintained by the Organisation in connection with its legitimate relationship with a Person or Community.OS.

37.6 Participant-Controlled Information

Participant-Controlled Information means information that Community.OS treats as belonging primarily to the Person's persistent identity or participant-controlled settings rather than solely to an Organisation record.

37.7 Personal Information

Personal Information has the meaning given under applicable privacy law.

37.8 Sensitive Information

Sensitive Information has the meaning given under applicable privacy law and may also include additional information that Community.OS treats as requiring heightened protection according to its privacy architecture.

37.9 Service Provider

Service Provider means an external provider selected by Sidekick Platforms to provide part of the Community.OS service.

37.10 Subprocessor

Subprocessor means an external provider engaged by one of our Service Providers to perform part of that provider's service where the term is relevant to the applicable contractual or regulatory context.

37.11 Terms

Terms means these Mosa Data Processing & Organisation Privacy Terms.

Data Processing & Organisation Privacy Commitment

Community.OS is unusual because the same Person may participate across many Organisations while remaining one persistent Person.

That makes the privacy relationship more sophisticated than:

Organisation owns customer database → software vendor processes it

Community.OS instead needs to preserve several different truths at once:

The Organisation legitimately stewards its own relationships and records.

The Person retains their persistent Mosa identity.

Sidekick Platforms operates the platform and has its own privacy responsibilities.

Information access remains contextual.

Technical capability does not create privacy authority.

Information should reveal itself when legitimately required, not simply because it exists.

Exports and integrations move responsibility with the information into the environment that controls the copy.

Service providers receive only what they need to perform their role.

Responsibility follows purpose, authority and meaningful control.

The goal is not to force every information relationship into one simplistic legal label.

The goal is to make it clear who is responsible for what, keep participant information appropriately protected as it moves through Community.OS, and ensure the trust model survives Organisations, integrations, external systems and future Community Spaces.