Privacy Policy

Updated: March 30, 2026

1. Introduction

This Privacy Policy explains how Sky Made Simple ApS ("we," "us," or "our") collects, uses, and protects personal data when you use the Implora platform ("Service").

Our Commitment: We are committed to protecting your privacy and complying with the EU General Data Protection Regulation (GDPR), the Danish Data Protection Act, and all applicable data protection laws.

2. Data Controller & Contact Information

Data Controller:

Sky Made Simple ApS

VAT: DK 43434527

Email: hello@implora.io

Website: https://implora.io

Data Protection Contact:

For data protection inquiries: hello@implora.io

Supervisory Authority:

Danish Data Protection Agency (Datatilsynet)

Website: https://www.datatilsynet.dk

Email: dt@datatilsynet.dk

3. Data We Collect

3.1 Account & Authentication Data

Microsoft Entra ID Information: Name, email address, job title, employer

Authentication Tokens: OAuth tokens for Entra ID B2B authentication

User Profile: User ID, tenant membership, group assignments

Legal Basis: Contractual necessity (GDPR Art. 6(1)(b))

3.2 Service Usage Data

Tenant Management: Tenant names, tenant IDs, consent records

Job Execution: Diagnostic runs, execution timestamps, job status

Reports: Generated reports and associated metadata

Legal Basis: Contractual necessity (GDPR Art. 6(1)(b))

3.3 Technical & System Data (Implora Portal Usage)

Data We Collect When You Use the Implora Portal:

Authentication Logs: Email address, user ID, login timestamps

IP Addresses: Source IP of portal access

Browser Data: User agent, browser type and version

Session Data: Access times, session duration, API calls

Device Information: Operating system, device type

Performance Data: Application Insights telemetry, error logs

Security Events: Failed login attempts, suspicious activity alerts

Purpose: System security, fraud detection, performance optimization, debugging

Legal Basis: Legitimate interests (GDPR Art. 6(1)(f)) - system security and performance optimization

Note: This section covers data collected from your direct use of the Implora portal. For data collected from Microsoft 365 tenants, see Sections 3.6-3.8.

3.4 Billing & Payment Data

Subscription Information: Plan type, billing cycle, subscription status

Payment Processing: Handled through Azure Marketplace or manual invoicing. We do not store payment card details.

Invoices: Billing history and payment records

Legal Basis: Contractual necessity (GDPR Art. 6(1)(b)) and legal obligation (GDPR Art. 6(1)(c)) - tax and accounting requirements

3.5 Tenant Microsoft 365 Data (Processed on Your Behalf)

When you run diagnostic tools:

Diagnostic Results: Security configurations, user counts, license usage

Microsoft 365 Metadata: Tenant information, service health data

Legal Basis: You are the Data Controller; we process this data as your Data Processor under our Data Processing Agreement (DPA)

3.6 Microsoft 365 Tenant Sign-In Logs & Security Data (Processed as Data Processor)

When you authorize Implora to generate security reports from Microsoft 365 tenants, we collect and process sign-in logs and authentication data for end users within those tenants.

Data Source: Microsoft Graph API (`auditLogs/signIns` endpoint)

Categories of Personal Data Collected (30-Day History):

Identity Information:

Email addresses (user principal names)

Full names (display names)

User unique identifiers

User types (member vs. guest users)

Sign-In & Access Data:

Timestamps of authentication attempts (30-day history)

IP addresses of sign-in locations

Geographic location data (country, city, state, GPS coordinates)

Success/failure status of each authentication

Application accessed (Exchange, SharePoint, Teams, etc.)

Device Information:

Device names and unique device IDs

Operating system and browser information

Device management status (Entra ID joined, hybrid, registered, unmanaged)

Device compliance and encryption status (BitLocker)

Trust type (workplace joined, personal device, etc.)

Authentication Methods & Security:

Multi-factor authentication (MFA) methods used per sign-in

Specific MFA types: SMS, authenticator app, FIDO2 security key, biometric

Passwordless authentication capability

Legacy authentication protocol usage (IMAP, POP3, SMTP)

Registered authentication methods per user (includes phone numbers if phone MFA is registered)

Risk & Behavioral Analytics:

Microsoft Identity Protection risk scores (low, medium, high)

Risk state and risk level assessments

Impossible travel detection (geographically improbable sign-ins based on time/distance)

Multi-country access patterns

Sign-in time patterns (business hours vs. off-hours)

VPN/proxy usage pattern detection

Conditional Access policy evaluation results

Purpose of Processing:

Generate security assessment reports analyzing sign-in patterns, risks, and anomalies

Detect potential security threats (unusual locations, failed authentication attempts, compromised accounts)

Identify compliance gaps (weak authentication, inactive users, risky behaviors)

Provide visibility into authentication activity and security posture

Authorization:

We only collect this data after you grant explicit OAuth consent through Microsoft Entra ID. Data collection begins only after consent is granted and ceases immediately if consent is revoked. You can manage consent permissions in your Microsoft Entra ID admin portal at any time.

Legal Basis:

You are the Data Controller for this data

Implora acts as Data Processor on your instructions under our Data Processing Agreement (DPA)

Legal basis is determined by you as Controller (typically: contractual necessity with your customers, legitimate interest in security monitoring, or compliance with legal obligations)

Data Retention:

Sign-in log data is collected as 30-day snapshots at report generation time

Retained within generated reports according to your subscription plan (typically 12 months)

Deleted within 30 days of report deletion or account termination

End User Rights:

End users whose data is collected from Microsoft 365 tenants should contact your organization (the data controller) to exercise GDPR rights. As Data Processor, we will assist you in responding to data subject requests.

3.7 External Collaborator Data (SharePoint Sharing Analysis)

When generating SharePoint sharing security reports, we collect data about external users who have been granted access to SharePoint sites, files, or folders.

Data Source: Microsoft Graph API (`sites`, `drives/items/permissions` endpoints)

Categories of Personal Data Collected:

External User Identity:

Email addresses of external collaborators

Display names

User IDs

Domains of external organizations

Guest account status

Access & Activity Data:

Last sign-in timestamps (correlates with Section 3.6 sign-in logs if external user has signed in)

Last non-interactive sign-in timestamps

Last successful sign-in timestamps

Number of sites/files accessed

Access count per external user

Sharing Metadata:

Files and folders shared with external users

Sharing link types (anonymous "Anyone" links vs. specific people)

Link expiration dates

Permissions granted (view, edit, etc.)

SharePoint site URLs

Purpose of Processing:

Identify external collaboration risks (anonymous sharing, expired links, overshared sensitive files)

Track external user access patterns

Assess data leakage risks through file sharing

Provide recommendations for secure external collaboration

Authorization:

We only collect this data after you grant explicit OAuth consent through Microsoft Entra ID. Data collection begins only after consent is granted and ceases immediately if consent is revoked. You can manage consent permissions in your Microsoft Entra ID admin portal at any time.

Legal Basis:

You are the Data Controller for external user data

Implora acts as Data Processor under our DPA

Legal basis determined by you (typically: legitimate interest in security monitoring, contractual necessity)

Data Retention:

Point-in-time snapshot at report generation

Retained within reports per subscription plan (typically 12 months)

Deleted within 30 days of report deletion or account termination

3.8 Organizational & Profile Data (Microsoft 365 Tenants)

When generating comprehensive security reports, we collect organizational and user profile information.

Data Source: Microsoft Graph API (`users`, `groups`, `organization` endpoints)

Categories of Personal Data Collected:

Organizational Information:

Department names

Job titles

Manager relationships

Office locations

Group memberships

License & Usage Data:

Assigned licenses (Microsoft 365, Entra ID, Intune)

License usage statistics (30-day activity reports)

Last sign-in timestamps (for inactive user identification)

Application usage patterns (Office 365 services accessed)

Password & Authentication Management:

Last password change timestamps

Password age calculations

Account creation dates

Account enabled/disabled status

MFA registration status

Purpose of Processing:

Identify inactive licensed users for cost optimization

Detect weak password hygiene (stale passwords)

Assess license utilization and compliance

Organizational structure analysis for security recommendations

Authorization:

We only collect this data after you grant explicit OAuth consent through Microsoft Entra ID. Data collection begins only after consent is granted and ceases immediately if consent is revoked. You can manage consent permissions in your Microsoft Entra ID admin portal at any time.

Legal Basis:

You are the Data Controller

Implora acts as Data Processor under our DPA

Legal basis determined by you (typically: contractual necessity, legitimate interest in cost optimization and security)

Data Retention:

Snapshot at report generation time

Retained within reports per subscription plan (typically 12 months)

Deleted within 30 days of report deletion or account termination

4. How We Use Data

4.1 Service Delivery

Authenticate users via Entra ID B2B

Execute diagnostic tools on authorized Microsoft 365 tenants

Generate and store security assessment reports

Manage tenant consent workflows

Track job execution and results

4.2 Service Improvement

Monitor system performance and reliability

Analyze usage patterns to improve features

Debug and resolve technical issues

Optimize diagnostic execution efficiency

4.3 Business Operations

Process subscription payments

Send service notifications and updates

Provide user support

Comply with legal obligations

4.4 Security & Fraud Prevention

Detect and prevent unauthorized access

Monitor for suspicious activity

Maintain audit logs for security investigations

Enforce multi-tenant data isolation

4.5 AI-Powered Features

AI features in Implora are opt-in. You can use the platform without enabling any AI functionality. When you use AI features, tenant data from Microsoft 365 - including security configurations, operational logs, and user identifiers such as email addresses and user principal names - may be transmitted to Anthropic (US-based) for analysis.

Purpose: Generate security insights, recommendations, and analysis based on tenant data

Legal Basis: Consent through opt-in use of AI features (GDPR Art. 6(1)(a)), or legitimate interests in providing AI-assisted security analysis (GDPR Art. 6(1)(f)) where opt-in constitutes voluntary use

Anthropic does not train its models on API data. See Sections 5.1 and 6.2 for transfer safeguards.

5. Data Sharing & Disclosure

5.1 Third-Party Service Providers (Data Processors)

We share data with trusted processors who assist in service delivery:

EU-Based Processors:

Microsoft Azure: Hosting, databases, blob storage, automation (Northern Europe region)

Dinero: Accounting software (receives organization names only for invoice records)

Application Insights: Performance monitoring and error tracking (EU region)

Dynamics 365 (Microsoft): CRM platform used to manage customer relationships. Data is synchronized from Intercom (companies, contacts, support cases) via Power Automate. Hosted in EU region.

Non-EU Processors:

Intercom: User support and engagement (US-based - see Section 6.2 for transfer safeguards)

Anthropic: AI analysis of tenant assessment data (US-based - see Section 6.2 for transfer safeguards)

Mailchimp (Intuit): Email marketing and service communications (US-based - see Section 6.2 for transfer safeguards)

All processors are bound by Data Processing Agreements (DPAs) and process data only on our instructions.

5.2 Microsoft 365 Tenants

We access Microsoft 365 tenants only with explicit OAuth consent

Data is processed to generate diagnostic reports

You remain the Data Controller for all tenant data

5.3 Legal Disclosures

We may disclose data when required to:

Comply with legal obligations, court orders, or government requests

Protect our rights, property, or safety

Prevent fraud or security threats

Enforce our Terms of Use

5.4 Business Transfers

In the event of a merger, acquisition, or sale of assets, your data may be transferred to the successor entity. We will notify you of any such change.

6. International Data Transfers

6.1 Primary Data Location

Data Center: Azure Northern Europe

All production data is stored within the EU

6.2 Transfers Outside EU/EEA

Intercom (US-based support platform):

We use Intercom for user support and engagement. Data transferred to Intercom is protected by:

EU-US Data Privacy Framework: Intercom is certified under the DPF

Standard Contractual Clauses (SCCs): As fallback mechanism if DPF is invalidated

Data Processing Agreement: GDPR-compliant DPA incorporated into service terms

Data minimization: Only necessary user data (name, email, support messages) is transferred to Intercom.

Anthropic (US-based AI provider):

We use Anthropic's Claude AI for AI-assisted analysis features. AI features are opt-in. Data transferred to Anthropic is protected by:

Standard Contractual Clauses (SCCs): EU-approved data transfer mechanism

No model training: Anthropic does not use API data to train its models.

Data deletion: Anthropic deletes API data within 30 days of processing.

When AI features are used, tenant data from Microsoft 365 - including security configurations, operational logs, and user identifiers such as email addresses and user principal names - may be transmitted to Anthropic.

Mailchimp (US-based email marketing platform):

We use Mailchimp for email campaigns and service communications. Data transferred to Mailchimp is protected by:

EU-US Data Privacy Framework: Mailchimp (Intuit) is certified under the DPF

Data Processing Agreement: GDPR-compliant DPA

Data minimization: Only name and email address are transferred for email communications.

Other transfers:

If data is transferred to other countries outside the EU/EEA, we ensure adequate safeguards:

Standard Contractual Clauses (SCCs): EU-approved data transfer mechanisms

Adequacy Decisions: Transfers to countries with EU-recognized adequate protection

Processor Agreements: All processors commit to GDPR-equivalent protections

6.3 Microsoft Azure Safeguards

Microsoft Azure processes data under:

Microsoft Data Processing Agreement (DPA): GDPR-compliant terms

EU Data Boundary: Commitment to store and process EU customer data within the EU

Standard Contractual Clauses: Available for international transfers if needed

Certifications: ISO 27001, ISO 27018, SOC 2

For details, see Microsoft's privacy commitments at: https://www.microsoft.com/trust-center

7. Data Retention

7.1 Active Accounts

Account Data: Retained while your subscription is active

Reports & Job History: Retained according to your subscription plan (typically 12 months)

Audit Logs: Retained for 24 months for security and compliance

7.2 Closed Accounts

Account Deletion: Within 30 days of termination (EU: 90 days maximum)

Backup Retention: Backup copies deleted within 90 days

Legal Holds: Data may be retained longer if required by law or legal proceedings

7.3 Billing Records

Invoices and payment records retained for 5 years (Danish bookkeeping requirements)

7.4 Microsoft 365 Tenant Data

Sign-In Logs & Security Data (Sections 3.6-3.8):

Collection: 30-day snapshots collected at report generation time

Report Retention: Retained within generated reports according to your subscription plan (typically 12 months)

Report Deletion: When you delete a report, associated Microsoft 365 data is deleted within 30 days

Account Termination: All Microsoft 365 tenant data deleted within 30 days of account closure

Backup Retention: Backup copies deleted within 90 days

Your Control: As Data Controller, you can request deletion of specific reports containing Microsoft 365 data at any time

Important: You (the customer organization) are the Data Controller for Microsoft 365 tenant data. Implora acts as Data Processor. You determine retention periods and deletion schedules according to your own data protection policies.

8. Your Data Protection Rights (GDPR)

Under GDPR, you have the following rights:

8.1 Right of Access (Art. 15)

You can request a copy of the personal data we hold about you.

8.2 Right to Rectification (Art. 16)

You can request correction of inaccurate or incomplete data.

8.3 Right to Erasure (Art. 17)

You can request deletion of your data ("right to be forgotten") when:

Data is no longer necessary for the purposes collected

You withdraw consent (where applicable)

You object to processing and there are no overriding legitimate grounds

Data was unlawfully processed

8.4 Right to Restriction (Art. 18)

You can request restriction of processing in certain circumstances.

8.5 Right to Data Portability (Art. 20)

You can receive your data in a structured, commonly used format and transmit it to another controller.

8.6 Right to Object (Art. 21)

You can object to processing based on legitimate interests.

8.7 Right to Withdraw Consent (Art. 7)

Where processing is based on consent, you can withdraw consent at any time.

8.8 Right to Lodge a Complaint (Art. 77)

You can file a complaint with the Danish Data Protection Agency (Datatilsynet):

Website: https://www.datatilsynet.dk

Phone: +45 33 19 32 00

Email: dt@datatilsynet.dk

8.9 Exercising Your Rights

To exercise any of these rights, contact us at: hello@implora.io

We will respond within 1 month (extendable to 3 months for complex requests).

9. Data Security

9.1 Technical Measures

Encryption: Data encrypted in transit (TLS 1.2+) and at rest (Azure Storage encryption)

Authentication: Entra ID B2B with multi-factor authentication support

Access Controls: Role-based access control (RBAC) and group-based permissions

Multi-Tenancy: Application-level data isolation by organization tenant ID

9.2 Organizational Measures

Security Training: Regular training for staff with data access

Access Restrictions: Least-privilege access principles

Incident Response: Security incident response procedures

Audit Logs: Comprehensive logging and monitoring

9.3 Vulnerability Management

Regular security assessments and penetration testing

Automated dependency scanning

Timely security patches and updates

9.4 Data Breach Notification

In the event of a data breach:

We will notify Datatilsynet within 72 hours (if required)

We will notify affected individuals without undue delay if high risk

We will document all breaches in our breach register

10. Cookies & Tracking

10.1 Essential Cookies

We use strictly necessary cookies for:

Session management and authentication

Security and fraud prevention

Service functionality

10.2 Analytics & Performance

Application Insights: Performance monitoring and error tracking

Legal Basis: Legitimate interests (GDPR Art. 6(1)(f))

10.3 Cookie Management

You can control cookies through your browser settings. Blocking essential cookies may impact service functionality.

11. Children's Privacy

The Service is not intended for individuals under 18 years of age. We do not knowingly collect data from children.

12. Data Processing Agreement (DPA)

12.1 Your Role as Data Controller

When you use the Service to process Microsoft 365 tenant data:

You are the Data Controller

We are the Data Processor

12.2 DPA Requirements

Our separate Data Processing Agreement (DPA) governs:

Processing instructions and limitations

Categories of data processed as Processor (including Microsoft 365 tenant sign-in logs, external collaborator data, and organizational profile data - see Sections 3.6-3.8)

Sub-processor authorizations

Data security obligations

Data subject rights assistance

Audit rights

Data breach notification procedures

12.3 Data Processing Agreement (DPA)

Our complete Data Processing Agreement (DPA) is available at: https://implora.io/legal/

The DPA includes:

GDPR Article 28 mandatory clauses

Data processing details and scope

Sub-processor list

Security measures

Data breach notification procedures

Data deletion and return processes

For questions about the DPA: hello@implora.io

12.4 Your Transparency Obligations as Data Controller

IMPORTANT: If you use Implora to generate security reports containing Microsoft 365 tenant data (Sections 3.6-3.8), you are the Data Controller for that data under GDPR.

Your Obligations under GDPR Article 14:

When you collect personal data indirectly (from Microsoft 365 tenants via Implora), you must inform the end users about the processing. This includes:

Information You Must Provide to End Users:

Your identity as Data Controller and contact details

Implora's role as Data Processor

Categories of personal data collected (sign-in logs, emails, IPs, device info, location data - see Sections 3.6-3.8)

Purpose of processing (security assessment, threat detection, compliance monitoring)

Legal basis for processing (e.g., legitimate interest in security, contractual necessity)

Retention period for reports and data

End user rights under GDPR (access, erasure, rectification, etc.)

How to exercise rights (contact information)

Data source (Microsoft 365 via Microsoft Graph API)

Timing Requirements:

Provide this information within 1 month of first collecting sign-in logs

Or at the time of first communication with end users

Or when the data is first disclosed to another recipient (whichever is earliest)

How to Comply:

Recommended Approaches:

Add disclosure to your customer onboarding documentation

Include in your organization's privacy policy or data processing notice

Provide notice through customer IT admin communications

Update employment/service agreements to include data processing disclosure

Display notice in customer tenant admin portals (if applicable)

What to Communicate:

"Your organization uses Implora (provided by Sky Made Simple ApS) to monitor and assess security in our Microsoft 365 environment. This includes collecting and analyzing sign-in logs (email addresses, IP addresses,

device information, location data, authentication details) from the past 30 days. This processing is necessary for detecting security threats, ensuring compliance, and protecting organizational data. Data is retained in security reports for up to 12 months. You have rights under GDPR to access, correct, or request deletion of your data. Contact [your organization's data protection contact] for more information."

Implora's Support:

We provide DPA templates and guidance documents to help you meet these transparency obligations. Contact hello@implora.io for:

Sample end user notification templates

GDPR Article 14 disclosure checklists

Data processing documentation assistance

13. Changes to This Privacy Policy

13.1 Updates

We may update this Privacy Policy to reflect:

Changes in our data processing practices

New legal requirements

Service enhancements

13.2 Notification

Material Changes: We will notify you via email or platform notice

Effective Date: Changes become effective 30 days after notification (unless legal requirements dictate otherwise)

Continued Use: Continued use after changes constitutes acceptance

14. Additional Rights for EU/EEA Residents

14.1 EU Data Act Rights

If you are located in the EU, you have additional rights under the EU Data Act:

Right to switch cloud providers with 2 months' notice

Right to data portability within 30 days

Protection from unfair contract terms

Right to interoperability and data access

14.2 ePrivacy Directive

We comply with the ePrivacy Directive and Danish implementing regulations regarding cookies and electronic communications.

15. Contact Us

For questions about this Privacy Policy or to exercise your data protection rights:

Sky Made Simple ApS

VAT: DK 43434527

Email: hello@implora.io

Website: https://implora.io

Data Protection Inquiries:

Email: hello@implora.io

Danish Data Protection Authority:

Datatilsynet

Borgergade 28, 5

1300 Copenhagen K

Denmark

Phone: +45 33 19 32 00

Email: dt@datatilsynet.dk

Website: https://www.datatilsynet.dk

Last Updated: March 30, 2026

By using the Service, you acknowledge that you have read and understood this Privacy Policy.