Records of Processing Activities (ROPA)

2 Sureños - GDPR Compliance Documentation

Document Version: 1.0
Last Updated: November 9, 2025
Responsible Party: 2 Sureños
DPO Contact: info@2surenos.pro

---

1. Executive Summary

This document fulfills the requirements of Article 30 of the GDPR (EU Regulation 2016/679) by maintaining comprehensive records of all personal data processing activities carried out by 2 Sureños through its website https://2surenos.pro.

---

2. Organization Details

Controller Information

- **Company Name:** 2 Sureños
- **Legal Form:** [To be specified]
- **Registration Number:** [To be specified]
- **Address:** Alicante, Spain
- **Contact Email:** info@2surenos.pro
- **Phone:** +34 711 509 180
- **Website:** https://2surenos.pro

Data Protection Officer (DPO)

- **Assigned:** No (not required for organizations under 250 employees without high-risk processing)
- **Privacy Contact:** info@2surenos.pro

---

3. Processing Activity #1: Contact Form Submissions

3.1 Purpose of Processing

- **Primary Purpose:** Process customer inquiries and quote requests for home improvement services
- **Legal Basis:**
- Consent (Article 6(1)(a) GDPR) - User explicitly consents via checkbox
- Legitimate Interest (Article 6(1)(f) GDPR) - Necessary to respond to service requests

3.2 Data Categories Collected

Personal Data

Data Type	Required	Storage Location	Encryption
Full Name	Yes	PostgreSQL Database	Yes (at rest)
Email Address	Yes	PostgreSQL Database	Yes (at rest)
Phone Number	Yes	PostgreSQL Database	Yes (at rest)
Postal Code	Yes	PostgreSQL Database	Yes (at rest)
Service Type	Yes	PostgreSQL Database	Yes (at rest)
Message/Description	Yes	PostgreSQL Database	Yes (at rest)
Submission Timestamp	Auto	PostgreSQL Database	Yes (at rest)
Submission Language	Auto	PostgreSQL Database	Yes (at rest)

Technical Data (Non-Personal)

- Browser type and version
- Operating system
- Referrer URL
- IP address (anonymized after 7 days)

3.3 Data Subjects

- **Categories:** Potential customers, existing customers, general inquirers
- **Geographic Scope:** Primarily Spain (Alicante region), European Union
- **Age Restrictions:** Only adults (18+ years) or parents/guardians acting on behalf of minors

3.4 Data Recipients

Internal Recipients

- Customer service team
- Service coordinators
- Management (for business analytics)

External Recipients

Recipient Type	Purpose	Location	Safeguards
Email Service Provider (SMTP)	Sending confirmation emails	EU/EEA	TLS encryption, GDPR-compliant
Database Provider (Abacus.AI)	Data storage and processing	EU/EEA-compliant	ISO 27001, encryption at rest/transit
Hosting Provider	Website infrastructure	EU/EEA-compliant	DPA in place, GDPR-compliant

3.5 Data Retention Period

- **Active Inquiries:** Until inquiry is resolved + 30 days
- **Completed Projects:** 6 years (legal requirement for invoicing/tax records)
- **Declined Inquiries:** 90 days, then anonymized
- **See Full Retention Policy:** [DATA_RETENTION_POLICY.md]

3.6 Data Security Measures

Technical Measures

- TLS 1.3 encryption for data in transit
- Database encryption at rest (AES-256)
- Secure authentication and access controls
- Regular security updates and patches
- Automated backup systems (encrypted)
- Rate limiting on form submissions (3-minute cooldown)

Organizational Measures

- Access control policies (least privilege principle)
- Staff training on data protection
- Incident response procedures
- Regular security audits
- Data processing agreements with all processors

3.7 International Data Transfers

- **Status:** No transfers outside EU/EEA
- **Future Transfers:** If required, only with adequate safeguards (Standard Contractual Clauses, adequacy decisions)

3.8 Data Subject Rights Implementation

- **Right to Access:** Via email to info@2surenos.pro (response within 30 days)
- **Right to Rectification:** Corrections processed within 7 days
- **Right to Erasure:** Honored within 30 days unless legal obligation requires retention
- **Right to Restriction:** Implemented via database flags
- **Right to Data Portability:** JSON/CSV format provided within 30 days
- **Right to Object:** Processed within 30 days

- **Withdrawal of Consent:** Immediate processing cessation

---

4. Processing Activity #2: Website Analytics & Cookies

4.1 Purpose of Processing

- **Primary Purpose:** Improve user experience, analyze website performance, optimize content
- **Legal Basis:** Consent (Article 6(1)(a) GDPR)

4.2 Data Categories Collected

Cookie Data

Cookie Name	Type	Duration	Purpose
cookieConsent	Technical	1 year	Store user’s cookie consent preference
preferred-language	Preference	1 year	Remember user’s language selection

Analytics Data (if implemented)

- Page views and navigation patterns
- Session duration
- Bounce rate
- Device and browser information (anonymized)

4.3 Data Subjects

- All website visitors

4.4 Data Recipients

- **Internal:** Website administrators, marketing team
- **External:** None (no third-party analytics currently implemented)

4.5 Data Retention Period

- **Cookie Consent:** 1 year (then re-requested)
- **Language Preference:** 1 year (then reset to default)
- **Analytics Data:** If implemented, max 14 months (aligned with GA4 standards)

4.6 Data Security Measures

- Cookies stored locally in browser (HttpOnly where applicable)
- No sensitive data stored in cookies
- Secure flag enabled for all cookies (HTTPS only)
- Cookie banner with clear opt-in mechanism

4.7 Data Subject Rights

- Users can revoke cookie consent at any time via the cookie policy page
- Browser settings allow manual deletion of cookies
- Clear instructions provided on cookie policy page

5. Processing Activity #3: Email Communications

5.1 Purpose of Processing

- **Primary Purpose:** Send service confirmations, respond to inquiries, provide quotes
- **Legal Basis:**
- Consent (Article 6(1)(a) GDPR)
- Contract Performance (Article 6(1)(b) GDPR)

5.2 Data Categories

- Email address
- Name
- Correspondence content
- Timestamps

5.3 Data Retention

- **Active Correspondence:** Duration of inquiry + 30 days
- **Contractual Emails:** 6 years (legal requirement)
- **Marketing Emails:** Until consent withdrawal (not currently implemented)

---

6. Data Breach Procedures

6.1 Detection and Assessment

- Immediate investigation within 24 hours of discovery
- Risk assessment to determine severity and impact on data subjects

6.2 Notification Requirements

- **Supervisory Authority:** Within 72 hours if risk to data subjects
- Spanish Data Protection Agency (AEPD): https://www.aepd.es
- **Data Subjects:** Without undue delay if high risk to rights and freedoms
- **Documentation:** All breaches recorded in breach register

6.3 Response Plan

1. Contain the breach immediately
2. Assess the scope and impact
3. Notify relevant parties (DPO, management, authorities)
4. Document the incident
5. Implement corrective measures
6. Review and update security procedures

---

7. Third-Party Processors

Current Processors

Processor	Service	Data Processed	DPA Status
Abacus.AI	Hosting & Database	All contact form data	Required ✓
SMTP Provider	Email delivery	Email addresses, names	Required ✓

Processor Requirements

- All processors must sign Data Processing Agreements (DPA)
- Regular audits of processor compliance
- Processors must demonstrate adequate security measures
- Notification requirements for sub-processors

---

8. Data Protection Impact Assessments (DPIA)

Current Status

- **DPIA Required:** No - Processing activities are low-risk
- **Reasoning:**
- No large-scale processing of sensitive data
- No automated decision-making or profiling
- No systematic monitoring
- No vulnerable data subjects

Trigger Events for DPIA

- Implementation of automated decision-making
- Large-scale processing (>10,000 individuals/year)
- Systematic monitoring of public areas
- Processing of special category data

---

9. Compliance Monitoring

Regular Reviews

- **Frequency:** Quarterly
- **Responsible:** Management + Privacy Contact
- **Checklist:**
- ✓ Review data inventory
- ✓ Update retention schedules
- ✓ Audit access logs
- ✓ Review processor compliance

- ✓ Test data subject rights procedures
- ✓ Update documentation

Annual Audit

- Comprehensive review of all processing activities
- Security assessment
- Staff training refresher
- Policy updates
- Documentation review

---

10. Training and Awareness

Staff Training Requirements

- Initial privacy training upon hiring
- Annual refresher training
- Training topics:
- GDPR principles and requirements
- Data handling procedures
- Security best practices
- Breach response procedures
- Data subject rights

---

11. Documentation and Record Keeping

Required Documentation

- ✓ This Records of Processing Activities (ROPA)
- ✓ Data Retention Policy
- ✓ Privacy Policy (published on website)
- ✓ Cookie Policy (published on website)
- ✓ Data Processing Agreements with processors
- ✓ Consent records (stored with contact form data)
- ✓ Data breach register (if applicable)
- ✓ Data subject rights request log

Retention of Documentation

- All compliance documentation: 6 years minimum
- Breach records: Indefinite retention

---

12. Contact and Questions

For questions about this document or data protection practices:

Email: info@2surenos.pro
Phone: +34 711 509 180
Website: https://2surenos.pro/politica-privacidad

For exercising data subject rights or complaints:
- Submit requests to: info@2surenos.pro
- Spanish Data Protection Authority (AEPD): https://www.aepd.es

---

13. Document Control

Version History

Version	Date	Changes	Author
1.0	2025-11-09	Initial creation	Management

Review Schedule

- **Next Review:** February 9, 2026
- **Review Frequency:** Quarterly
- **Trigger Events:** New processing activities, legal changes, incidents

---

Appendices

Appendix A: Data Flow Diagram

```
User → Website Form → Database (Encrypted) → Customer Service Team
                    ↓
               Email Service → User Confirmation
```

Appendix B: Legal Basis Mapping

- **Contact Forms:** Consent + Legitimate Interest
- **Cookies:** Consent
- **Email Communications:** Consent + Contract Performance
- **Invoice/Tax Records:** Legal Obligation

Appendix C: Supervisory Authority Contact

Agencia Española de Protección de Datos (AEPD)
- Website: https://www.aepd.es
- Phone: +34 901 100 099
- Address: C/ Jorge Juan, 6, 28001 Madrid, Spain

Document End