

1. Purpose

This addendum defines how Ecosafe ensures the protection of personally identifiable information (PII) when processed by cloud services, software-as-a-service platforms, or third-party suppliers, in compliance with ISO 27001:2022 A.5.36.

2. Scope

Applies to all personal data processed externally by:

- Cloud-based software platforms (e.g., Simpro)
- Reporting and data warehouse services that hold copies of data from those platforms (e.g., Tugger)
- Subcontractors, suppliers, and other service providers
- Any external processor handling PII on behalf of Ecosafe

3. Identification & Approval

- All third-party processors are identified, assessed, and approved before engagement.
- Approval includes consideration of:
 - PII sensitivity
 - Security controls
 - Legal and contractual obligations
 - Whether the customer contract requires the customer's prior approval of the processor or subcontractor

4. Contractual & Legal Requirements

- Contracts or SLAs with third parties explicitly include:
 - Confidentiality and security obligations
 - Incident reporting requirements
 - Retention and secure disposal of PII
 - Compliance with GDPR and relevant privacy legislation

5. Risk Assessment & Monitoring

Issue: 2	Change Note No: CNN-0083	Review Due: October 2027
Author: F.Sweetman	Created Date: 07/01/2026	
Approved By: A.Marston	Classification: Internal Use Only	

- Risk assessment is performed for all outsourced PII processing, considering:
 - Data sensitivity
 - Supplier location (including cross-border transfers)
 - Potential threats or vulnerabilities
- Ongoing oversight includes:
 - Periodic supplier review and audit where appropriate
 - Confirmation that PII protection measures remain effective
 - Integration with incident management for reporting breaches

6. Record-Keeping

- A PII inventory is maintained to show:
 - Category of PII processed
 - Responsible processor or cloud service
 - Purpose of processing
 - Retention period
- Inventory is updated whenever new PII is outsourced or systems change.
- The PII inventory is held at Appendix A.
- Where PII cannot be handled in line with the Data Protection Policy (ES-POL-010) or the Records Protection & Retention Policy (ES-POL-045), the exception is recorded at Appendix B with its scale, the reason, the controls applied and the date it ends. Exceptions are reviewed at least every six months by the General Manager.

7. Integration with ISMS

- Existing ISMS controls for access management, backups, incident response, and BCP apply equally to outsourced/cloud PII.
- Non-compliance or incidents involving third-party processors are escalated according to the Information Security Incident Response process.

8. References

- ISO 27001 Annex A – A.5.36 Protection of PII in outsourced/cloud processing
- (ES-POL-010) Data Protection Policy
- (ES-POL-045) Records Protection & Retention Policy
- (ES-POL-022) Data Breach Policy

Signed:

Issue: 2	Change Note No: CNN-0083	Review Due: October 2027
Author: F.Sweetman	Created Date: 07/01/2026	
Approved By: A.Marston	Classification: Internal Use Only	

Adam Marston
CEO
Dated: 22/10/2026

Issue: 2	Change Note No: CNN-0083	Review Due: October 2027
Author: F.Sweetman	Created Date: 07/01/2026	
Approved By: A.Marston	Classification: Internal Use Only	

Appendix A – PII Inventory

Rows marked “to confirm” are to be completed by the system owner by the next review (April 2027). Further systems (for example HR and payroll) are to be added by the General Manager.

System / processor	Category of PII	Purpose	Ecosafe role	Retention
Simpro – contact fields	Resident names, addresses, telephone numbers, email addresses; access and vulnerability notes	Appointments, access, delivery of works, complaints	Processor for the customer	12 months after job completion, then removed (ES-POL-010 s7)
Simpro – job records	Property address, works completed, certificates, operative names	Contract record, defects, certification, legal claims	Processor (resident-related); controller (own records)	6 years (ES-POL-045)
Simpro – free-text fields (historic)	Resident and customer-staff contact details; some health and vulnerability information	None – recorded in error	Processor for the customer	Exception – see Appendix B (PII-EX-001)
Tugger reporting warehouse	Copy of Simpro and Xero data, including job free-text fields	Management reporting	Ecosafe's processor (sub-processor for customer data)	Mirrors source. Records deleted in Simpro are kept in the warehouse with a deleted flag – purge arrangement to confirm with provider
Xero	Customer and supplier contacts, subcontractor payment details	Finance and accounting	Controller	6 years (ES-POL-045)
Microsoft 365 (Outlook, SharePoint, Teams)	Emails and documents containing resident, employee and supplier data	Communication and document storage	Controller; processor for resident data	Emails 2–6 years; documents per ES-POL-045
Subcontractors	Resident contact and access details for allocated jobs	Delivery of works	Sub-processor engaged by Ecosafe	Delete on job completion – written confirmation to obtain

Issue: 2	Change Note No: CNN-0083	Review Due: October 2027
Author: F.Sweetman	Created Date: 07/01/2026	
Approved By: A.Marston	Classification: Internal Use Only	

Issue: 2	Change Note No: CNN-0083	Review Due: October 2027
Author: F.Sweetman	Created Date: 07/01/2026	
Approved By: A.Marston	Classification: Internal Use Only	

Appendix B – PII Exception Record

Field	Detail
Reference	PII-EX-001
Title	Historic resident contact data held in Simpro job free-text fields
Date raised / owner	21/10/2026 – General Manager
Status	Open – approved; actions in progress
Description	Resident names, telephone numbers and email addresses have been entered into job description and notes fields on completed Simpro jobs, rather than in the designated contact fields. In some records these entries also describe a resident's health or vulnerability (for example mobility or hearing), which is special category data. Some entries are contact details of customer staff, which are also personal data.
Scale	The initial estimate was about 1,000 jobs. A sample of completed jobs in Simpro (via the Tugger warehouse, 21/10/2026) indicates the true number is materially higher. Jobs with a UK phone number or email address in the description or notes field: September 2022 – 574 of 1,062 completed jobs; September 2025 – 289 of 986; September 2026 – 228 of 1,220; March 2019 and March 2021 – 20 each. Applied across the 92,128 completed jobs (2017–2026), this suggests in the region of 12,000–20,000 affected jobs, concentrated in jobs completed from 2022 onwards. This is an estimate from pattern matching and must be confirmed by a full count before the record is finalised.
Customers affected	Largest in the September 2026 sample: BCP Council, Aster Group, Southern Housing, Adur District Council, Winchester City Council and Stonewater, with smaller numbers across around ten other customers. A full breakdown by customer is to be produced with the full count.
Why the data cannot be removed	Advice received is that Simpro does not allow text in these fields to be removed from a completed job without deleting the whole job record. Editing these fields through the Simpro API has not yet been tested; this is an open action.
Why deleting the whole job is not proportionate	The job record is needed to evidence the works completed, to support defect and warranty claims, to hold certificates and reports, to meet customer contract requirements and to defend legal claims. ES-POL-045 sets a 6-year retention for job certificates and reports. Deleting the job would remove records Ecosafe and its customers have a legitimate need to keep.

Issue: 2	Change Note No: CNN-0083	Review Due: October 2027
Author: F.Sweetman	Created Date: 07/01/2026	
Approved By: A.Marston	Classification: Internal Use Only	

Field	Detail
Controls to reduce the risk	1. From the date of approval, contact data is recorded only in designated fields (ES-POL-010 s7), supported by a staff briefing and monthly spot checks of new jobs. 2. Restrict access to completed jobs in Simpro to roles that need it (to be confirmed as achievable in Simpro security groups). 3. Do not share historic job descriptions or notes with subcontractors. 4. Exclude job description and notes fields from routine reports and exports produced from the Tugger warehouse. 5. Inform the affected customers (as data controllers) of the issue and the agreed approach. 6. Test, on a small sample with written sign-off, whether the free-text fields can be edited through the Simpro API. If so, replace this exception with a clean-up plan. 7. Delete in full, subject to checks, jobs already past the 6-year retention period (see below).
Date the issue ends	The exception ends for each job when it reaches the 6-year retention period and is deleted in full. Assuming no new free-text entries after the enforcement date, the last affected job reaches this point in October 2032. 18,292 jobs were completed before 21/10/2020 and are already beyond the 6-year retention period in ES-POL-045. These should be scheduled for deletion now, after checking for open claims and any longer retention in customer contracts. Matching deletions must also be purged from the Tugger warehouse.
Next review	April 2027 (six-monthly)
Approved by / date	F.Sweetman – 22/10/2026

Issue: 2	Change Note No: CNN-0083	Review Due: October 2027
Author: F.Sweetman	Created Date: 07/01/2026	
Approved By: A.Marston	Classification: Internal Use Only	