Appendix 1: Our retention periods for data and AI

The following table outlines standard data retention periods based on data categories, aligned with principle of the General Data Protection Regulation (GDPR) and ISO/IEC 27001 AND 27701 standards. These retention periods serve as general guidance and may be adjusted based on legal requirements, contractual obligations or specific risk requirements.

Data Category (if applicable)	Example	Typical Retention Period
User account data	Names, email addresses, authentication credentials	Active use + up to 2 years after account closure
Additional notes:	In line with GDPR principles of storage limitation (Art. 5(1)(e)) and ISO 27001 Annexes for identity management.	
Operational or log data	System logs, access logs, performance records	12-24 months
Additional notes:	Retained for security, audit, and incident response per ISO 27001, limited to necessity under GDPR.	
Personal identifiable information	Names, addresses, ID numbers, contact details	Until purpose is fulfilled or consent withdrawn
Additional notes:	Must be deleted or anonymised when no longer necessary as per GDPR, limited to relevant data subject rights.	
Financial or transactional data	Invoices, payment records, tax-related information	6-10 years (jurisdiction dependent)
Additional notes:	Required for legal compliance and aligns with ISO 27701 and GRPR articles.	
AI training data	Text, images, or behaviour used in model training	Varies (*see caveat)
Additional notes:	Once data in integrated into trained models, removal may not be technically feasible/possible.	

Aggregated or anonymised data	Statistical trends, usage patterns, synthetic datasets	Indefinite
Additional notes:	GDPR does not apply to anonymised data, permitted under ISO 27701 if re-identification is impossible.	
Contractual or legal documents	Agreements, consent records, NDAs, compliance findings	Duration of contract + up to 6 years
Additional notes:	Retained for evidence, defence of legal claims as per GDPR and covered under ISO 27701.	

*Data that has been used to train AI models may not be removable on an individual basis after training is complete. This depends on the technical architecture of the AI system (e.g., where the model stores representations of individual data points). Where feasible, we apply data minimisation, differential privacy, or anonymisation techniques prior to training. However, we acknowledge that full deletion of data influence from a trained model may not be practical or even possible in some circumstances.