Keepabl Crosswalk to LOCS:23 UK GDPR Standard

Crosswalk created by Keepabl Ltd against LOCS:23 v12.2, as at 18 December 2023

Key:	Support
	Strong Support

#	Title	Control Reference	Control Objective	UK GDPR Ref	Audit Ref	Keepabl SaaS	Keepabl Pack
8.1	**Organisational and Client File Governance**						
8.1.1	Privacy Council	LOCS:23:C1 Governance - Privacy Council	To form an internal governance body to oversee Client File data protection.	Art 5(2)	LOCS:23:A1 Privacy Council	UK ICO Accountability Framework	
8.1.2	Data Protection Officer	LOCS:23:C2 - DPO	To appoint a single point of contact responsible for day-to-day duties associated with the protection of Client File data.	Art 5(2), Arts 37-39	LOCS:23:A2 –DPO	UK ICO Accountability Framework	
8.1.3	ICO Registration and Cooperation	LOCS:23:C3 - Registration	Mandatory registration and cooperation with the ICO	Art 5(2)	LOCS:23:A3 – ICO Registration	UK ICO Accountability Framework	
8.1.4	Data Protection Principles	LOCS:23:C4 - Principles	To ensure that core Data Protection principles are applied to the processing of Client data.	Art 5(1) Art 5(2)	LOCS:23:A4 – Principles	UK ICO Accountability Framework, Gap Analysis, Reporting	Full Privacy Policy Pack
8.1.5	Data Protection and Information Security Policy	LOCS:23:C5 – Data Protection and Information Security Policy	To document and distribute a Data Protection Policy to provide staff with enough direction to understand their roles and responsibilities regarding data protection and information governance.	Art 5(1)(f), Art 5(2)	LOCS:23:A5 – Data Policy Document	File Library	Full Privacy Policy Pack
8.1.6	Business Continuity Plan	LOCS:23:C6 – BC Policy	To document how the Client File is protected in the event of a serious incident impacting the live data.	Art 5(1)(f)	LOCS:23:A6– BC Policy Document	File Library	Business Continuity & Disaster Recovery Procedure
8.1.7	Retention & Destruction Policy	LOCS:23:C7 – R&D Policy	To document the length of time Client File data will be retained and the process for its safe destruction when no longer required.	Art 5(1)(e)	LOCS:23:A7– R&D Policy Document	Data Map, Art 30 Records	Retention Policy & Procedure
8.2	**Data Subject Rights**						
8.2.1	Transparency & Communication	LOCS:23:C8 –Transparency & Communication	To provide the required communication to the Data Subject within required timescales when rights are invoked.	Art 11-12, Art 23	LOCS:23:A8– Transparency & Communication	Rights Management, Data Map, Activity Analysis	DSR Policy & Procedure
8.2.2	Right to be informed	LOCS:23:C9 – Right to be informed	To be transparent as to the processing of a Data Subject's data and make all relevant information available.	Art 13-14, Art 23	LOCS:23:A9 – Right to Information	Rights Management, Data Map, Activity Analysis	DSR Policy & Procedure
8.2.3	Right of Access	LOCS:23:C10 – Right of access	To enable the Right of Access and provide the Data Subject with access to their processed Personal Data.	Art 15, Art 23	LOCS:23:A10– Right of access	Rights Management, Data Map, Activity Analysis	DSR Policy & Procedure
8.2.4	Right to Rectification	LOCS:23:C11 – Right of Rectification	To enable the Right of rectification and enable the Data Subject to amend, complete or remedy any incorrect or incomplete Personal Data.	Art 16, Art 19, Art 23	LOCS:23:A11– Right of Rectification	Rights Management, Data Map, Activity Analysis	DSR Policy & Procedure
8.2.5	Right to Erasure	LOCS:23:C12 – Right of Erasure	To enable the Right of Erasure and enable the Data Subject to have Personal Data deleted.	Art 17, Art 19, Art 23	LOCS:23:A12– Right of Erasure	Rights Management, Data Map, Activity Analysis	DSR Policy & Procedure
8.2.6	Right to Restriction of Processing	LOCS:23:C13 – Right to Restriction of Processing	To enable the Right to Restriction of Processing and enable the Data Subject to have Processing restricted in certain circumstances.	Art 18-19, Art 23	LOCS:23:A13– Right to Restriction of Processing	Rights Management, Data Map, Activity Analysis	DSR Policy & Procedure
8.2.7	Right to Data Portability	LOCS:23:C14 – Right to Portability	To enable the Right to Portability and enable the Data Subject to have data ported to another Organisation.	Art 20, Art 23	LOCS:23:A14 – Right to Portability	Rights Management, Data Map, Activity Analysis	DSR Policy & Procedure
8.2.8	Right to Object	LOCS:23:C15 – Right to Object	To enable the Right to Object and enable the Data Subject to stop their data being processed.	Art 21, Art 23	LOCS:23:A15 - Right to Object	Rights Management, Data Map, Activity Analysis	DSR Policy & Procedure
8.2.9	Right not to be subject to automated decision making	LOCS:23:C16 – Automated Decision Making	To enable the Right to not have automated decision making.	Art 22, Art 23	LOCS:23:A16 – Automated Decision Making	Rights Module, Data Map, Activity Analysis	DSR Policy & Procedure

Keepabl Crosswalk to LOCS:23 UK GDPR Standard

Crosswalk created by Keepabl Ltd against LOCS:23 v12.2, as at 18 December 2023

Key:	Support
	Strong Support

#	Title	Control Reference	Control Objective	UK GDPR Ref	Audit Ref	Keepabl SaaS	Keepabl Pack
8.3	**Operational Policy**						
8.3.1	Data Protection by Design and Default	LOCS:23:C17 – Design & Default Privacy	To ensure that data protection is built in to activities relating to the processing of Client File data.	Art 25	LOCS:23:A17 – Default Privacy	Privacy Framework, Benchmarks, Data Map, Assessment Management	Policy and Procedure on DPIAs, LIAs and Transfers
8.3.2	Risks and Data Protection Impact Assessment (DPIA)	LOCS:23:C18 - DPIA	To ensure that any potential risks to Client File data are assessed when introducing new or modified Processing activities	Art 35-36	LOCS:23:A18 – DPIA	Data Map, Risk Map, Assessment Management	Policy and Procedure on DPIAs, LIAs and Transfers
8.3.3	Processing Records	LOCS:23:C19 - ROPA	To document all Processing activities related to the Client File	Art 30	LOCS:23:A19 – ROPA	Data Map	
8.3.4	Lawful Processing	LOCS:23:C20 – Lawful Processing	To determine, justify and document the lawful basis for Processing Client data.	Art 6-7, Art 9-10	LOCS:23:A20 – Lawful Processing	Data Map, Activity Analysis	Data Protection Policy
8.3.5	Personal Data Breach Management	LOCS:23:C21 –Personal Data Breach Management	To ensure that any breach to the confidentiality, integrity or availability of Data Subject data is managed.	Art 33-34	LOCS:23:A21 – Personal Data Breach Management	Breach Management	Personal Data Breach Policy & Procedure
8.3.6	Data Subject Rights Management	LOCS:23:C22 – Data Subject Rights Management	To ensure that any Data Subject request to invoke a right is managed.	Art 15-22	LOCS:23:A22 – Data Subject Rights Management	Rights Management	DSR Policy & DSR Procedure
8.3.7	Technical Security Measures	LOCS:23:C23 – Technical Security Measures	To provide technical security measures for protecting Client File data.	Art 5(f), Art 32	LOCS:23:A23– Technical Security Measures		
8.3.8	Organisational Security Measures	LOCS:23:C24 – Organisational Security Measures	To provide Organisational security measures for protecting Client File data.	Art 5(f), Art 32	LOCS:23:A24 – Organisational Security Measures		
8.3.9	Data Protection Training	LOCS:23:C25 – Training	To ensure continued protection of the Client File through training as to data protection best practice.	Art 5(2), Art 39	LOCS:23:A25 – Training		
8.4	**Third Party Service Providers and Data Sharing**						
8.4.1	3rd Party Supplier Register	LOCS:23:C26 - Supplier Register	To document all Third Parties that supply services relating to the processing of Client File data.	Art 5(2)	LOCS:23:A26 - Supplier Register	Data Map, Vendors, Entities	Vendor (Processor) Policy & Procedure
8.4.2	Supplier Status Assessment	LOCS:23:C27 – Supplier Status	To determine whether a Third Party service provider is a Data Controller, Joint Controller or a Data Processor.	Art 24, Art 26, Art 28, Art 29, Art 31	LOCS:23:A27 – Supplier Status	Data Map, Vendors, Entities	Data Protection Policy, Vendor (Processor) Policy & Procedure
8.4.3	Supplier Risk Assessment	LOCS:23:C28 – Supplier Risk Assessment	To determine whether a Third Party Data Processor provides required data protection.	N/A	LOCS:23:A28 – Supplier Risk Assessment	Data Map, Vendors, Entities	Vendor (Processor) Policy & Procedure
8.4.4	Controller to Processor and Processor to Processor Relationships	LOCS:23:C29 – C-P and P-P Data Sharing	To outline the Organisations requirements for Client File data protection in a Data Processing Agreement.	A28, A29	LOCS:23:A29 – C-P Relationships		Template Data Processing Agreement
8.4.5	Controller to Controller Data Sharing Relationships	LOCS:23:C30 – C-C Data Sharing	To outline the Organisations requirements for Client File data protection in a Data Sharing Agreement.	Art 5(2), Art 26	LOCS:23:A30 – C-C Data Sharing		Template Data Sharing Agreement
8.4.6	Transfer of Personal Data outside of the UK	LOCS:23:C31 – Cross Border Data Transfer	To outline the Organisations requirements for Client File data protection when sharing across borders.	Art 44-47, Art 49	LOCS:23:A31 – Cross Border Data Transfer		Transfers Policy
8.4.7	Legal Service Providers not located in the UK	LOCS:23:C32 – NON-UK Service Providers	To ensure UK representation for Clients whose data is processed by a non-UK domiciled service provider.	Art 27	LOCS:23:A32 – NON-UK Service Providers	Transfers Management	
8.5	**Monitor & Review**						
8.5.1	Internal Audit Process	LOCS:23:C33 – Internal Audit Process	To ensure that the Organisation is applying LOCS standards to the Client File.	Art 5(2)	LOCS:23:A33 – Internal Audit Process	Full Privacy Management Software	Full Privacy Policy Pack
8.5.2	Internal Audit Review	LOCS:23:C34 – Internal Audit	To ensure that applied data protection measures are in place and effective.	Art 5, Art 24	LOCS:23:A34 – Internal Audit Review	Full Privacy Management Software	Full Privacy Policy Pack