cinnamon digital applications

Cinnamon Digital Applications

GDPR Self-Assessment

cinnamon digital applications

Contents

cinnamon digital applications

Overview

This document is the GDPR self-assessment results for Cinnamon Digital Applications Limited. The assessment is reviewed annually as part of our GDPR compliance processes.

Version:	1.0
Version Superseded:	-
Owner:	William Aspinall, Director and Data Protection Officer
Date issued:	22nd March 2018
Review date:	1 year from date issued
Target audience:	Company wide

cinnamon digital applications

Part 1 Documentation

1. Information you hold	
1.1 Your business has conducted an information audit to map data flows.	
	Not yet implemented or planned
	Partially implemented or planned
✓	Successfully implemented
	Not applicable
Evidence	
• Information audit completed. • Appointment of Data Protection Officer. • Information Asset Register completed. • Data Flow Mapping completed • Risk assessment and monitoring for each Asset and Mapping completed.	

cinnamon digital applications

Part 2 Accountability and Governance

2.1 Accountability	
Your business has an appropriate data protection policy.	
	Not yet implemented or planned
	Partially implemented or planned
✓	Successfully implemented
	Not applicable
Evidence	
• Information Security policy in place. • Policy sets out company approach to data protection and responsibilities for implementing the policy and monitoring compliance. • Policy approved by company Board of Directors • Policy available to all staff • Policy reviewed every 12 months or otherwise dependent on changes to legislation.	

2.2 Data Protection Officer	
Your business has a nominated a data protection lead or Data Protection Officer (DPO).	
	Not yet implemented or planned
	Partially implemented or planned
✓	Successfully implemented
	Not applicable
Evidence	
• Data Protection Officer appointed.	

cinnamon digital applications

Part 2 Accountability and Governance (cont)

2.3 Management Responsibility	
Decision makers and key people in your business demonstrate support for data protection legislation and promote a positive culture of data protection compliance across the business.	
	Not yet implemented or planned
	Partially implemented or planned
✓	Successfully implemented
	Not applicable
Evidence	
• All staff trained in NHS Information Governance and Cyber Security • Managers regularly review GDPR documents e.g. Information Asset Register	

2.4 Information risks and data protection impact assessments	
Your business manages information risks in a structured way so that management understands the business impact of personal data related risks and manages them effectively.	
	Not yet implemented or planned
	Partially implemented or planned
✓	Successfully implemented
	Not applicable
Evidence	
• Joint risk assessments with all customers (data controllers) • Data Protection Officer responsible for review, recording and mitigation of all risks • Privacy Impact Assessments (PIA) conducted for all contracts	

cinnamon digital applications

Part 2 Accountability and Governance (cont)

2.5 Data protection by design	
Your business has implemented appropriate technical and organisational measures to show you have considered and integrated data protection into your processing activities.	
	Not yet implemented or planned
	Partially implemented or planned
✓	Successfully implemented
	Not applicable
Evidence	
• SQL Database pseudonymisation of identifiable information when appropriate • Use of encryption as standard in all applications • SSL for all applications and websites • Microsoft Identity Framework used to manage accounts, roles and logins	

2.6 Training and awareness protection by design	
Your business provides data protection awareness training for all staff.	
	Not yet implemented or planned
	Partially implemented or planned
✓	Successfully implemented
	Not applicable
Evidence	
• All staff trained in GDPR • All staff trained in Cyber Security • All staff trained in Information Governance • Above training mandatory every 12 months for all staff	

cinnamon digital applications

Part 2 Accountability and Governance (cont)

2.7 The use of sub-processors	
Your business has sought prior written authorisation from the data controller before engaging the services of a sub-processor.	
	Not yet implemented or planned
	Partially implemented or planned
	Successfully implemented
✓	Not applicable
Evidence	
• Cinnamon Digital Applications does not use sub-contractors to process data on our behalf.	

2.8 Operational base	
If your business operates outside the EU, you have appointed a representative within the EU in writing.	
	Not yet implemented or planned
	Partially implemented or planned
	Successfully implemented
✓	Not applicable
Evidence	
• Cinnamon Digital Applications does not operate outside of the EU or the UK. All company operations are conducted in the UK. This includes all data processing activities.	

cinnamon digital applications

Part 2 Accountability and Governance (cont)

2.9 Breach notification	
Your business has effective processes to identify, report, manage and resolve any personal data breaches.	
	Not yet implemented or planned
	Partially implemented or planned
✓	Successfully implemented
	Not applicable
Evidence	
• Data breach process outlined in the company Information Security Policy. • A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This means that a breach is more than just losing personal data. • All suspected breaches must be reported at once to the Data Protection Officer. The company will notify the customer within 24 hours and the Information Commissioner Office within 72 hours if that breach is likely to result in a risk to the rights and freedoms of individuals.	

cinnamon digital applications

Part 3 Individual Rights

3.1 Right of access	
Your business has a process to respond to a data controllers request for information (following an individuals' request to access their personal data).	
	Not yet implemented or planned
	Partially implemented or planned
✓	Successfully implemented
	Not applicable
Evidence	
• Process for subject access requests outlined in the company Subject Access Request Policy. • Cinnamon Digital Applications is committed to providing an efficient and transparent process and service to our customers, their lawful representatives and organisations who have lawful authority to access records.	

3.2 Right to rectification and data quality	
Your business has processes to ensure that the personal data you hold remains accurate and up to date.	
	Not yet implemented or planned
	Partially implemented or planned
✓	Successfully implemented
	Not applicable
Evidence	
• All staff are responsible for the accuracy of the data they record and use. All data should be accurate and up-to-date. • Process for subject access requests outlined in the company Subject Access Request Policy.	

cinnamon digital applications

Part 3 Individual Rights (cont)

3.3 Right to erasure including retention and disposal	
Your business has a process to routinely and securely dispose of personal data that is no longer required in line with agreed timescales as stated within your contract with the data controller.	
	Not yet implemented or planned
	Partially implemented or planned
✓	Successfully implemented
	Not applicable
Evidence	
• All information assets owned or processed by the company will be recorded on the Information Asset Register. The Data Protection Officer will be responsible for the security of that asset. • All information assets must be maintained until the end of their useful life and then must be disposed of safely and without risk to the organisation, or the organisation's patients, clients and staff. • All computer equipment will be disposed of by The Data Protection Officer in accordance with industry standards, EU and UK environmental and health and safety regulations. A record of all disposals will be maintained. • All contracts to contain standard clauses covering erasure, data retention and disposal.	

cinnamon digital applications

Part 3 Individual Rights (cont)

3.4 Right to restrict processing	
Your business has procedures to respond to a data controllers' request to supress the processing of specific personal data.	
	Not yet implemented or planned
	Partially implemented or planned
✓	Successfully implemented
	Not applicable
Evidence	
• Process for managing the supression of specific personal data outlined in the company Information Security Policy. • Individuals have a right to block or restrict the processing of personal data. • The data controller may request that the company restrict the processing of specific in accordance with GDPR.	

3.5 Right of data portability	
Your business can respond to a request from the data controller for the supply of the personal data you process in an electronic format.	
	Not yet implemented or planned
	Partially implemented or planned
✓	Successfully implemented
	Not applicable
Evidence	
• Process for subject access requests outlined in the company Subject Access Request Policy. • Cinnamon Digital Applications is committed to providing an efficient and transparent process and service to our customers, their lawful representatives and organisations who have lawful authority to access records. • The company will provide all requests for digital data in a structured format e.g. CSV to the data controller in an agreed timescale.	

cinnamon digital applications

Part 4 Data Security

4.1 Security Policy	
Your business has an information security policy supported by appropriate security measures.	
	Not yet implemented or planned
	Partially implemented or planned
✓	Successfully implemented
	Not applicable
Evidence	
• Process for managing information security is outlined in the company Information Security Policy.	

cinnamon digital applications

Contact Details

Cinnamon Digital Applications Limited

Email: support@cinnamondigitalapplications.co.uk
www.cinnamondigitalapplications.co.uk

UK Company Number: 11128319
ICO Registration Number: ZA331005