Healthy London Partnership

The Data Controller Console and GDPR Features

Nov 2018

V2

Supported by and delivering for London's NHS, Public Health England and the Mayor of London

Introduction

The Data Controller Console (DCC) is an online system that makes it easier for organisations to manage their sharing agreements and makes it more efficient for care organizations to share information with each other by tracking, recording and reporting on information sharing and the subsequent agreements. The console also makes the process of creating, agreeing and updating information agreements easier thus reducing cost and burden on organisations hosting the information sharing agreements.

The DCC also helps organisations to address some of the General Data Protection Regulation (**GDPR**)/ Data Protection Act 2018 requirements. This document sets out the features of the DCC and indicates how the features supports organisations' GDPR compliance:

DCC Features	Description	GDPR	Status
Organisational Profile	Organisations will be able to create their own profiles so that other organisations can share with confidence the following information is captured; - Type of Organisation - Borough's serviced - Services provides - ICO number - IG Toolkit - Caldicott Guardian - Data Privacy Officer (DPO) - Contact Details Data Privacy Officer - Qualifications/Scores: CQC…. etc The DCC has functionality to support data sharing or flows authentication enabling organisations to authenticate processing activity and also comply with technical organisational security measures	**Articles 30 (a & b)** - records of processing activities require organisations to provide names and contact details of the DPO and the purpose of processing **Article 37** - The controller or the processor shall publish the contact details of the data protection officer and communicate them to the supervisory authority **Article 38** - Data subjects may contact the data protection officer with regard to all issues related to processing of their personal data and to the exercise of their rights under this Regulation	Available
Upload & Track ISA	Information Sharing Agreements can be uploaded, stored and tracked. Organisations can invite other organisations to join or can make their ISA available so other organisations can request to join.	**Article 30** - Records of processing activities	Available

	The three ISA Features are; **1. Create ISA** – upload and create ISA **2. ISA Management**- Summary and information on all ISA's you are participating in **3. ISA Registry** – Summary table plus information on ISA's you are hosting		

Data Processing Contracts	Organisations can upload existing contracts and contact information of processors and attach them with ISA held within their organisations in the DCC or ISA that they are participating in hosted on other organisations.
	
	Types of contracts that can be uploaded are;
	
	    - Data Processing Agreements
	    - Data Processing Contracts
	    - Service Level Agreements
	    - Data Processing Deed
	
	Contracts will supply data controllers with the contact details of processing organisation in case of a breach
		Article 28 - Processor
		
		Article 29 - Processing under the authority of the controller or processor
			Available

Data Protection Impact Assessments	Data Protection Impact Assessment (DPIAs) helps organisations to identify the most effective way to comply with their data protection obligations. They are also an integral part of taking privacy by design approach and are mandatory in the new GDPR guidance. DCC Features;	**Article 24 (1) -** Responsibility of the controller **Article 25** - Data Protection by design **Article 30** - Record of processing activities **Article 32.** 1 - Security of	Available

	- Digital DPIA template based on ICO guidance – **Technology, Processing, People** approach - Ability to upload DPIA PDF if required - DPIA Attached to every ISA hosted - Ability to see DPIA of ISA you are participating in - Ability to add Risks to DPIA	processing **Article 35.** 7 (c & d) - Data Protection Impact Assessment **Article 47** - Binding Corporate Rules	
Audit and Reporting	Ability for users to run and export reports based on their roles; - Audit activity on DCC - Reports on ISA, hosted and participating - DPC's – hosted and attached to ISA's (hosted and participating in) - Configure reports on Data Flows in excel format	**Article 5(1) (f)** –Technical and organisational security measures (TOSM).	Available
Data Sharing Tab	As part of GDPR guidance organisations need to map their data flows in order to assess their privacy risks. The DCC will have the basic ability to view their Information sharing arrangements (including DPIAs) across London via and interactive map, using filters, the following are examples of filters used; - ISA - DPCs to ISAs - ISAs with DPIA's - Type of information shared - Type of organisation sharing with	**Article 25** - Data protection by design and by default **Article 30 (c)** - Records of processing activities, description of categories of data subjects and categories of personal data **Article 35** (4 & 5) - Data protection impact assessment, have a public list of the processing operations	Available Further enhancements will be released in December 2018

	Organisations will be able to pull off Excel spread sheets with selected information presented		
HIE Profile	The DCC will provide a unique profile for organisations hosting local STP Health Information Exchange's (HIEs). This will allow organisations to set security rules and report on data processing.	**Article 5(1)(f)** – Technical and organisational security measures (TOSM).	To be released in December 2018
Local Authority Alignment	Adults and Children's social care which are part of Local Authorities regularly partner and share vital information with NHS organisations to provide care for citizens. The DCC has been aligned to meet the internal needs of recording vital information about the organisations so all can confidently share such as; - Ability to add separate Caldicott Guardian for Adult and Children - Capture professional scores such as OFSTED - Ability to call out and define services they provide	**Article 5(1)(f)** – Technical and organisational security measures (TOSM).	Available

| Public Facing Website | Being transparent and providing accessible information to individuals about how you will use their personal data is a key element of the Data Protection Act 1998 (DPA) and the EU General Data Protection Regulation (GDPR). The most common way to provide this information is in a privacy notice.

The dedicated website will de-burden the care organisations by providing a central public repository for fair processing notices, ISA's, Organisation Details. The Public Facing website for London will be hosted on https://www.myhealth.london.nhs.uk/

Features include;

- User friendly visual representation of information sharing across London
- Dedicated website with Map of London, citizens can select and filter information they want to see
- Information on ISA's, Organisations, Fair Processing Notices and Privacy Officer contact details sourced from publishable information in DCC
- Fair Processing Notice's to detailed and links to be made available when uploading ISA's in DCC, press publish, then pulled through to website
- Maps of data sharing if you search for an organisation on the webpage
- Map of London, using key for different orgs | **Article 6** - Lawfulness of processing

Article 9 - Processing of special categories of personal data

Article 12 - Transparent information, communication and modalities for the exercise of the rights of the data subject

Article 13 - Information to be provided where personal data are collected from the data subject

Article 14 - Information to be provided where personal data have not been obtained from the data subject | To be released October 2018 |

E-ISA	Create an electronic ISA template for data controllers to use in the DCC, this will cut down on paper and increase standardisation which is an historic problem for Information sharing. Features of the e-ISA - Ability to specify data being shared to either category or more granular via a Data Directory - Easy use standard template - Ability to support joint data controllers' model-including ability to review and collaborate - Attach PDF or e-DPIA - Associate DPC's etc. - Information to be easily pulled through on public facing website - E-ISA exportable to PDF	**Article 30** – Records of processing activities **Article 40** (g) - Codes of conduct, the protection of children and consent re parental responsibility **Article 57** 1 (b) - Tasks, re public awareness and risks to processing activities specifically to children	In development – to be released December 2018
Data Directory	Ability to upload data templates or use national standard templates from the Professional Record Standards Board (PRSB), making it easier to set up data sharing within ISA's. This will be the first stage in the development of an extensive standardised the data directory for London,	**Article 9** - Processing of special categories of personal data **Article 25** - Data Protection by design **Article 20** - Right to data portability	
Controlling Data Flows	Data Controllers will have the ability to authenticate data flows for their organization based on sharing arrangement information held in the DCC via ISAs, DPCs, Data Directory, DPIAs - Confidentiality rules engine based on most up to date national guidance	**Article 30** - Records of processing activities **Article 40** 2(i) - Codes of conduct, notification of personal breaches	In development – to be released March 2019

	- Authentication of data flow by SIRO, Caldicott Guardians to support interoperability engines - Audit functionality added - Ability to support granular sharing		
Social Care Organisations	Social Care organisations such as Care Homes are vital partners to delivering care The DCC will aim to support and engage private organisations that are part of care communities, providing a standard and transparent way to enable information sharing arrangements (ISA and DPIA templates) with health and social care organisations.	**Article 5(1)(f)** – Technical and organisational security measures (TOSM).	Released in December r