Spindle
Document Capture

GDPR Guidance

The information contained on this page is for general guidance purposes only. It should not be taken for, nor is it intended as, legal advice. We would advise customers to seek their own legal advice if they are unsure about the implications of the GDPR on their businesses.

1. Introduction

This document is intended to assist you with your GDPR compliance requirements by explaining what type of data is typically processed by users of Spindle Document Capture (SDC) and how that data is processed by you as a “Controller” of that personal data. This will assist you with ensuring your records are compliant with GDPR. Draycir are neither the Controller nor Processor of any personal data held in Spindle Document Capture.

Should you have any questions that cannot be clarified within this document please contact our Support Desk via email on support@draycir.com

2. The purposes of your processing

As a Controller it is up to you to determine the purpose for which you are processing personal data but Spindle Document Capture is typically used for the following purposes:

- The provision and management of customer financial and accounting documentation;
- The provision and management of supplier financial and accounting documentation.

3. A description of the categories of individuals and categories of personal data

Spindle Document Capture has the ability to hold the following categories of personal data:

- **Server Administrator > User Profiles** – Ability to add/edit/remove users that require / have access to Spindle Document Capture. Personal data collected are: Name and Email address. This information is the minimum level required in order to ensure that Spindle Document Capture is able to track and record user activities within the software.
- **Server Administrator > System Configuration > Mobile Administration** – requires the users email address so that Spindle Document Capture has the ability to manage mobile device users (add/remove devices) that require & have access to Spindle Document Capture.
- **Pending Tray/Document Search/Document Archive** – Displayed the Name of the user that has uploaded the document. Documents – The primary purpose of Spindle Document Capture is to allow the archival of documents (currently to a file system location), where there is no restriction on the type of documents that can be archived. The documents themselves may contain personal data.
- **Metadata** – Documents archived in Spindle Document Capture can be assigned metadata (for document searching purposes). The metadata could contain personal data e.g. sole trader names or contact information, however this information is configurable and within your control.

4. Recipients of personal data

Spindle Document Capture is a self-contained software application, therefore personal data is not automatically shared with any organisation other than the licensed user of the software.

5. Data Transfers outside the EU

Spindle Document Capture does not automatically transfer any data outside the EU unless you specifically choose to send that data to a third party located outside the EU.

6. Retention schedules

Spindle Document Capture only stores the personal data identified in Section 3 and retains this information for your security and auditing purposes. Currently there is no automated scheduling in place to delete or purge personal data. Therefore you should determine the retention period that is appropriate to your circumstances and apply these accordingly.

Regarding documents archived in Spindle Document Capture, although there is no control on the types of document archived, it is expected that the software will be used to store financial / accounting records which may contain personal data which are critical for HMRC purposes. Spindle Document Capture allows the ability to protect documents for retention periods determined by the user. There is a default setup of 6 years, as the required retention period set out by HMRC is 6 years plus current year, otherwise known as 6 years + 1.

7. Technical and organisational security measures

Spindle Document Capture is installed on your on-premise systems and therefore overall security measures are as per your general information security policies. However, please note that the software uses Microsoft Windows Authentication when logging into Spindle Document Capture, so Spindle Document Capture does not store the user's username and password, however all connection strings are encrypted to ensure any application interacting with Spindle Document Capture is authorised to do so.

DRAYCIR®