

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 GDPR and other data protection laws on their businesses.

1. Introduction

This document is intended to assist you with your GDPR compliance requirements by explaining what type of personal data of users Spindle Purchase Invoice Recognition (SPIR) is typically processing and how such personal data may be processed by you acting as a "Controller" and Draycir acting as a "Processor" (including other sub-processors). This may assist you in ensuring that your records are compliant with GDPR, however you must also make your own assessments.

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, SPIR is typically used for the following purposes:

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

Also, it is up to you as the Controller to determine as to what lawful basis you wish to rely upon to process the user's personal data.

3. A description of the types of personal data

SPIR has the ability to hold the following types of personal data:

- **Server Administrator > User Profiles** – Ability to add/edit/remove users that require / have access to SPIR. Personal data collected are: Name and Email address. This information is the minimum level required in order to ensure that SPIR is able to track and record user activities within the software.
- **Document Portal/Document Search/Document Archive** – Display the Name of the user that has uploaded the document.
 - The users Windows Security Identifier (SID) is also recorded and stored. This information is required in order to identify the user's name when archiving the document into the ERP
- **Documents** – The primary purpose of SPIR is to allow the posting of Purchase Invoice data into the ERP and archiving the associated documents to a location on-premises. These documents themselves may contain personal data.
- **Metadata** – Documents archived via SPIR will be associated metadata (for document searching purposes). The metadata could contain personal data e.g. sole trader names or contact information.

4. Recipients of personal data

Personal data collected within SPIR, may be shared with other Draycir products to enhance functionality, for example SPIR can be configured to integrate with Spindle Approvals to approve Purchases Invoices.

Personal data may be processed by other sub-processors such as, Draycir Thailand and/or Canon IRIS, to help diagnose issues and improve the recognition of purchase invoice data.

5. Data Transfers outside the EEA

SPIR does not automatically transfer personal data outside the EEA. In order to improve our services or provide additional support, some personal data may be transferred outside the EEA to our subsidiary company Draycir Thailand. However, such transfer would be subject to an approved Data Processor Agreement.

6. Retention schedules

GDPR requires Controllers to keep personal data no longer than is necessary. Documents containing personal data will be stored in the Document Portal until deleted by the user, where any personal data is deleted by the user it is stored for a further period of 30 days for backup, audit and compliance purposes.

Once a document has been archived using Spindle Document Capture (SDC) service 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. Please refer to the SDC GDPR compliance guidance for more information on the SDC retention schedules.

Upon cancellation, termination or non-renewal of the contract, any personal data in the Document Portal is retained for 90 days before such data is deleted.

7. Technical security measures

SPIR is a cloud-based solution built on Microsoft Azure services. Microsoft Azure have over 90 compliance offerings, where more information around compliance can be found on the Microsoft Azure website:

<https://azure.microsoft.com/en-gb/overview/trusted-cloud/compliance/> All our Microsoft Azure services and data are hosted in a secure Data Centre within the European Union (EU), where access to any of the resources are restricted to key personnel requiring multi factor authentication.

All data is encrypted at rest and is securely transferred using Transport Layer Security (TLS) so that the content of the communication cannot be understood if intercepted. Where the data can only be accessed via a secure authentication mechanism. Access to this data is audited and monitored for threat detection.

Draycir considers its security measures to be appropriate under the GDPR. Draycir also performs regular auditing of assets in Microsoft Azure to ensure that best practices are maintained and security features of products and services used are enabled