Spindle Document Distribution Cloud

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 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 is typically processed by users of Spindle Document Distribution Cloud 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 but Spindle Document Distribution Cloud is typically used for the following purposes:

- The provision and management of financial and accounting information / documentation;
- The provisioning of PayThem links via payment service providers.

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

- Spindle Document Distribution Cloud has the ability to hold the following types of personal data:
- Account identification data – such as: username and password. This information is required in order to securely access the Spindle Document Distribution Tools.
- User Settings – Ability to add/edit the current list of users and configure users default; email, fax and CRM device, when distributing documents.
- Email Settings – Can specify the recipients of the email and override the sender's details.
- Fax Settings – Can specify the recipients of the fax and override the sender's details.
- CRM integration – Connection details in the form of a username and password will be stored on an encrypted basis.
- 3rd Party Database Integration – Connection details will be stored on an encrypted basis.
- PayThem – Spindle Document Distribution provides the facility for end users to add a clickable button on the generated invoice, to allow customers to pay invoices using a Payment Provider such as; Opayo (formally Sage Pay), WorldPay, Stripe and TranSafe. The recipient's name, address and email address are required in order to provide this service.
- Audit Logs – Captures all activities within the software when distributing documents. The default setting overwrites the audit logs each time a document is distributed, however there is the ability to disable this feature so that the logs are recorded for every distributed document.

4. Recipients of personal data

- Personal data collected within Spindle Document Distribution Cloud, may be shared with other Draycir products/services or service providers to provide functionality, for example with the Payment Provider via the PayThem function.
- Personal data may be processed by other sub-processors such as, Draycir Thailand, to help diagnose issues.

5. Data Transfers outside the EEA

Spindle Document Distribution Cloud does not automatically transfer personal data outside the EEA unless you specifically choose to send that data to a third party located outside the EEA.

For PayThem, the Payment Provider you choose to use, may transfer data outside of the EEA in providing the functionality to you. Please check their applicable service terms or privacy notices.

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. Cloud repository

Spindle Document Distribution Cloud stores personal data identified in Section 3 (with the exception of Audit Logs) within the Spindle Document Distribution Cloud database. A local copy of this database will reside on each individual user's workstation or server. When using Spindle Document Distribution Cloud in a user environment (not on a shared server), in order for changes to be synchronised across all of your users, a copy of the Spindle Document Distribution Cloud database is stored in Draycir's cloud repository (hosted by Microsoft Azure in the EU). When a configuration change is made in Spindle Document Distribution Cloud Tools from a specific workstation, this database is uploaded to Draycir's cloud repository and then filtered down to every other user's workstation to ensure all users have the very latest updates.

+44 (0)116 255 3010 sales@draycir.com draycir.com

DRAYCIR®

PayThem data is also stored in Draycir's cloud repository (hosted by Microsoft Azure in the UK or EU) to allow payments to be made via the PayThem payment portal. Note: Draycir does not hold bank or card payment details. These are solely managed by the payment provider you choose to use with this service.

7. Retention schedules

As Spindle Document Distribution Cloud requires this data to be able to provide the service, there is no automated scheduling in place to delete or purge personal data from the database either on-premise or in the cloud repository. The data is retained in the cloud repository until you cease to use the relevant software or service. If you do not wish your data to be held in the cloud repository you would need to cease to use Spindle Document Distribution Cloud and obtain an alternative license option from Draycir. Should you wish for your data to be removed from Draycir's cloud repository, please let us know via support@draycir.com.

In respect of PayThem - data is retained to provide the payment facility and to maintain an audit history of payments. If you do not wish for your data to be held in the cloud repository, you would need to cease to use PayThem. Should you wish for your data to be removed from PayThem, please let us know via support@draycir.com.

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.

8. Technical security measures

Spindle Document Distribution Cloud is installed on your systems (other than the cloud repository described above) and therefore overall security measures remain with you and as per your general information security policies. However, please note that the software is set to enforce secure encryption of all user passwords as well as all connection strings so that any application interacting with Spindle Document Distribution Cloud is authorised to do so.

For PayThem, the transactional information that is held is securely encrypted so that the data being transferred to the Payment Provider cannot be intercepted and misused. Please refer to the Payment Provider's service terms or privacy notices for details on what security measures are taken by the Payment Provider.

As mentioned in section 6, the Spindle Document Distribution Cloud data is uploaded to a cloud repository built on Microsoft Azure services. Microsoft Azure have over 90 compliance certifications, including ISO 27001, 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 secure Data Centres, 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 applicable data protection legislation. 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.