



Informationsblatt gemäß Artikel 3 EU Data Act

Verbundener Dienst: e-BRIDGE Capture & Store workflow +
Hersteller: Scanshare Applications
Anbieter: Toshiba TEC Germany Imaging Systems GmbH

1. Klassifikation

Gemäß den Definitionen des EU-Datenschutzgesetzes (Verordnung 2023/2854):

- Vernetztes Produkt: ein physischer Gegenstand, der Daten über seine Nutzung oder seine Umgebung erfasst, generiert oder sammelt und in der Lage ist, diese Daten über einen elektronischen Kommunikationsdienst zu übermitteln.
- Zugehöriger Dienst: ein digitaler Dienst, einschließlich Software, der in ein vernetztes Produkt integriert oder mit diesem verbunden ist und für dessen Betrieb, Reparatur oder Wartung erforderlich ist.

Bewertung des Dokumenten Navigators:

Produktname	Typ	Bewertung
e-BRIDGE Capture&Store	Verwandte Dienstleistung	e-BRIDGE Capture & Store ist eine Softwarelösung, die auf vernetzten Multifunktionsdruckern (MFPs) ausgeführt wird oder mit diesen interagiert. Sie gilt als damit verbundener Dienst im Sinne des Datengesetzes. Sie gilt selbst nicht als „vernetztes Produkt“, kann jedoch Daten verarbeiten, die von solchen Geräten stammen.

2. Dokumentation zur Datenpolitik

Als Anbieter einer entsprechenden Dienstleistung ist e-BRIDGE Capture & Store verpflichtet, eine Datenschutzerklärung vorzulegen, in der Folgendes festgelegt ist:

- Welche Daten abgerufen, verwendet und generiert werden
- Zu welchen Zwecken sie verarbeitet werden
- Wie Nutzer auf die Daten zugreifen können
- Informationen zur Weitergabe oder Übermittlung



Die e-BRIDGE Capture & Store Richtlinie zur Datenerfassung und -speicherung (CSDP) schreibt vor, dass Organisationen personenbezogene Daten respektieren und schützen müssen – unabhängig davon, wohin diese übertragen, verarbeitet oder gespeichert werden.

3. Das Engagement von Scanshare für die CSDP-Bereitschaft

Scanshare hat es sich zur Aufgabe gemacht, seinen Kunden und Partnern innovative Lösungen für Datenschutz, Sicherheit und Governance anzubieten, um sie auf ihrem Weg zur Einhaltung der CSDP-Vorschriften zu unterstützen. Die Anwendungen von Scanshare speichern oder übermitteln keinerlei personenbezogene Daten.

Obwohl die Anwendung zur Erstellung von Workflow-Prozessen genutzt wird, in denen personenbezogene Daten verarbeitet werden können, werden diese Daten nicht außerhalb des Workflow-Prozesses übertragen.

4. Vertrauen der Daten

Daten und deren Schutz gewinnen für den Einzelnen und die Gesellschaft zunehmend an Bedeutung. Unternehmen müssen sich das Vertrauen der Öffentlichkeit in ihre Fähigkeit zum verantwortungsvollen Umgang mit Informationen verdienen. Innerhalb der Scanshare-Anwendung liegt es in der Verantwortung des Erstellers des Workflows, die gesetzlichen Vorschriften zum Umgang mit Daten einzuhalten (z. B. bei der Anbindung an Anwendungen von Drittanbietern im Zusammenhang mit der Speicherung personenbezogener Daten). Bei der Nutzung des Anwendungsprotokolls, der allgemeinen Einstellungen und des Dateispeichers können einige personenbezogene Daten lokal in der Anwendung gespeichert werden. In allen drei Fällen besteht die Möglichkeit, alle lokal gespeicherten personenbezogenen Daten zu löschen (Löschen von Protokollen, Zurücksetzen von Einstellungen, Löschen von Daten aus dem Speicher).

Eine Ausnahme bildet die Funktion „Bericht erstellen“, bei deren Ausführung möglicherweise personenbezogene Daten verwendet werden. Der Nutzer wird jedoch bei der Nutzung dieser Funktion darauf hingewiesen und erklärt sich damit einverstanden, dass diese Daten zu Supportzwecken an uns oder den Anbieter übermittelt werden; die Übermittlung der Daten zu diesem Zweck muss manuell veranlasst werden (es erfolgt keine automatische Datenübermittlung).

Im Rahmen seines CSDP-Projekts verstärkt Scanshare sein kontinuierliches Engagement für „Privacy by Design“. Scanshare arbeitet daran, Datenschutzgrundsätze noch stärker in seine Geschäftsprozesse zu integrieren, mit dem Ziel, dass technische und organisatorische Sicherheitsmaßnahmen standardmäßig die Menge und Verwendung personenbezogener Daten auf das unbedingt erforderliche Maß beschränken. Diese Maßnahmen werden auch die bereits bestehenden Kontrollen zur Beschränkung des Zugriffs auf personenbezogene Daten verstärken, unter anderem in Bezug auf mobile Anwendungen, die auf sinnvolle Standardeinstellungen setzen, um zu verhindern, dass personenbezogene Daten versehentlich an Dritte weitergegeben werden.