SCANDIT

Scandit Data Transmission Specification as of June 1st, 2026
(older versions available at https://ssl.scandit.com/terms-archive)

Scandit Data Transmission Specification

Depending on the license key settings selected in the Order Form, certain data from the Software may be transmitted to Scandit. The following table outlines the categories of data that may be transmitted, including potential transmission of personally identifiable information (PII). The scope of data transmission depends on the analytics configuration associated with the license key, as specified in the order form.

Without “Analytics” (as selected in the Order Form)	Depending on the license key settings selected in the Order Form, following types of data may be transmitted to Scandit from the Software for debugging, statistical analysis, performance monitoring, improvements and/or license compliance purposes: o Installation Identifier - generated by the Software, distinguishes installations of the Software o License Key identifier - generated by the Software, distinguishes the license key used by the Software o Software version - Software version number o Application identifier - name of the App (inserted in the Order Form Scope table) with which the Software is integrated, such as "myapp.customer.com" o Scan count - number of scans that the Software performs o Device model - the device model on which the Software runs (e.g. "iPhone 14") o Operating system and version - the operating system and version on which the Software runs, e.g. iOS 15.1. o IP address - the IP address used to establish Internet connection
With “Analytics” (as selected in the Order Form)	In addition to above, the following information is transmitted to Scandit for debugging, statistical analysis, performance monitoring, improvement, and license compliance purposes: o Scan engine and device status information - parameters of the decoding process, i.e. Software performance (e.g. scan and decode speed, barcode type scanned, crash logs) o Scan engine results - the data decoded by the Software (e.g. data encoded in a barcode)

Specific Data Transmission Specifications for Barcode and Label Scanning products

Data types transmitted for processing as part of Product Functionality

Where Cloud Fallback is enabled in your license key, the following data types may be transmitted for processing:

Product	**Feature**	**Transmitted Data**
Barcode, MatrixScan and Smart Label Capture	Cloud Fallback	Scan images are transmitted to Scandit's cloud for inference. The Software returns extracted label data (e.g. expiry date, address).

Specific Data Transmission Specifications for ID Scanning products

The above Data Transmission Specification also applies to Scandit's ID scanning products. Depending on the license key settings, this might include Personally Identifiable Information (PII) being transmitted to Scandit.

The following tables outline the specific conditions under which identity-document data, including Personally Identifiable Information (PII), is or is not transmitted to Scandit:

Data types transmitted as part of Analytics

Analytics Information	**Feature**	**Transmitted Data**
Scan engine and device status information	Scanning of MRZ, VIZ or PDF417 on identity document	Document type, issuing jurisdiction, document version, issuing and expiry year/month, hashed or anonymized barcode content, and structural information of barcode.
	ID Validate for MRZ ,VIZ and PDF417 scans	Includes the result of the verification: authentic / fake.
Scan Engine Results	Scanning of MRZ or VIZ on identity document	Scans of a machine readable zone (MRZ) or visual inspection zone (VIZ), will not transmit personal data from the identity document as part of the scan engine result mentioned in the table above.
	ID Validate for MRZ and VIZ scans	Scans of a MRZ or VIZ may transmit personal data from the identity document as part of the scan engine results when verifying the authenticity of the identity document based on a comparison of the data encoded in the barcode and the data printed in the MRZ or VIZ.
	Scanning of PDF417 barcode on identity document	Scans of a PDF417 code may transmit personal data from the identity document as part of the scan engine results mentioned in the table above. Scan engine results of US driver licenses may include the data encoded in the PDF417 code, as

		defined in the AAMVA DL/ID standard for US driver licenses. Scan engine results of PDF417 codes of other identity documents may include the data encoded in the code, as defined by applicable standards.

Purpose of Data Collection in Analytics (ID Scanning details):

1. The purposes of debugging, statistical analysis, performance monitoring, improvements in the case of ID documents include the following: improvements by proactively identifying new ID formats and fixing customer issues without customers having to collect the data and share it with us, as well as product improvements for certain document types;
2. (ID Validate only) Customer reporting on prevalence of fake identity documents based and debugging of the fake classification.

Data types transmitted for processing as part of Product Functionality

Please note that for ID scanning of VIZ/MRZ and PDF417 barcodes, all data processing happens on device, and data is only transmitted as part of analytics. For ID Validate and ID Bolt, data might be transmitted for processing:

Product	**Feature**	**Transmitted Data**
ID Validate	Verification of ID documents via ID Scanning SDK for the Web or ID Bolt.	Verification of US driver licenses and identity cards with a barcode as specified by the American Association of Motor Vehicle Administrators transmit personal data as part of the verification when using the ID Scanning SDK for the Web or ID Bolt. Data transmitted as part of the verification of US driver licenses and identity cards when using ID Scanning SDK Web or Bolt may include the data encoded in the PDF417 code, as defined in the AAMVA DL/ID standard for US driver licenses
ID Validate	Verification of ID documents via ID Scanning SDK Native.	Verification on the ID Scanning SDK Native only transmits personal data from the document as part of the scan engine results

		(i.e. only when license key settings in the order form specifies “Analytics”).
ID Bolt	Device Handover	Scanning of an ID can be performed on other devices than the device that initiated the ID scan process (“Device Handover”). In this case, personal data from the identity document from scans of a MRZ, VIZ or PDF417 will be transmitted through Scandit’s servers. Scandit does not store any personal data from the identity document transmitted this way and all personal data is encrypted end to end without Scandit servers having access to the data (zero-knowledge encryption).