Annex to Scandit Software License and Services Agreement: Data Processing Agreement

Depending on the license key settings selected in the Order Form, certain data from the Software may be transmitted to Scandit. Please review the Order Form for the license key settings and see below for the description of such data. If no specific license key settings are selected in the Order Form, then all the data set out below will be transmitted to Scandit.

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)*

To the extent any data is transmitted to Scandit, Scandit will use the data for the above purposes. Scandit will make data available to the Company in the Dashboard for reporting purposes (e.g. number of installations and scans). If applicable, the Company shall ensure, and hereby grants to Scandit, the rights and licenses necessary for the above purposes. If the data includes any personal data, the below data processing agreement applies.

*** For ID Scanning products, please see also the technical note**

Data Processing Agreement

1. These data protection terms and conditions apply to the processing of personal data, if any, by Scandit for the Company in accordance with the Software License and Services Agreement in which these terms are referenced. For capitalized terms not defined here, please see the Software License and Services Agreement.
2. To the extent Scandit processes personal data for the Company, Scandit will process such personal data as necessary to provide Scandit’s products and services to the Company as per the Agreement.
3. Scandit products and services may transmit personal data to Scandit. Scandit will process such personal data for as long as the products and services are used by any (App) users. This may be after the date of termination of the Agreement and will include the period required to dispose of the data after the products and services are no longer used. Scandit may retain anonymized data after the termination of the Agreement for product development purposes.
4. Scandit will ensure that it has in place appropriate technical and organizational measures to protect against unauthorized or unlawful processing and against accidental loss or destruction of, or damage to, personal data. Such measures must be appropriate to the harm

that might result from the unauthorized or unlawful processing or accidental loss, destruction or damage and the nature of the data, having regard to the state of technological development and the cost of implementing the measures.

5. Scandit will assist the Company at the Company's cost, in responding to any request from a data subject in relation to the Agreement and in ensuring compliance with the Company's obligations under applicable data protection laws with respect to security, breach notifications, impact assessments and consultations with supervisory authorities or regulators.
6. Scandit will ensure that any person Scandit authorizes to process personal data protects the personal data in accordance with these terms and Scandit's confidentiality obligations under the Agreement.
7. When use of Scandit products and services ceases, personal data will no longer be transmitted to Scandit and Scandit will, within a reasonable period, dispose of all personal data in its possession (except where required by law to keep it).
8. If Scandit becomes aware of any accidental, unauthorized or unlawful destruction, loss, alteration, or disclosure of, or access to the personal data, Scandit will promptly notify the Company. Scandit will provide the Company with a detailed description of the incident and the identity of each affected data subject with periodic updates. Scandit will also provide any other information the Company may reasonably request in relation to such an incident.
9. Provided that Scandit imposes data protection terms on any sub-processor that are significantly equivalent to these terms and that Scandit remains liable for any breach by a sub-processor of these terms, the Company hereby authorizes Scandit to engage sub-processors to process personal data. Scandit will notify the Company of any changes to sub-processors reasonably in advance to allow the Company to object to such changes. If the Company objects and the parties fail to find a workable solution, Scandit may terminate the Agreement. Current sub-processor list is available at https://www.scandit.com/privacy.
10. Scandit will only transfer personal data outside the EEA if Scandit has complied with its obligations under applicable data protection laws to ensure adequate safeguards.
11. Scandit will maintain complete and accurate records and information to demonstrate its compliance with the applicable data protection laws and these terms and allow for audits of such records and information by the Company or its designated auditor solely for the purpose of checking Scandit's compliance with these terms. Such an audit is at the Company's expense and not more than once per year except where required by a relevant regulatory authority or law. The Company must provide reasonable prior written notice to Scandit, including an audit plan. Audits must not materially interfere with Scandit's business operations. Auditors shall comply with Scandit's security policies. Prior to such an audit, Scandit may, at its option, provide the Company with a report verifying Scandit's compliance with these terms. Having reviewed the report, the Company shall only request an audit if the Company has reasonable and demonstrable grounds to believe the measures described in the report to be insufficient.

Product specific technical data for ID Scanning products

1. Data types transmitted as part of Analytics:

    1.1. 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. However, in the ID Validate edition, 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.

    1.2. 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.

    1.3. Scans of a MRZ, VIZ or PDF417 code may transmit the following data as part of the scan engine and device status information mentioned in the table above: document type, issuing jurisdiction, document version, issuing and expiry year and month, hashed or anonymised barcode content and structural information of barcode. In case of ID Validate, this will also include the result of the verification: authentic / fake.

2. Data types transmitted as part of products with ID Validate and ID Bolt:

    2.1. As part of ID Validate Edition, 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. 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”).

    2.2. As part of the ID Bolt, 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.

3. The purposes of debugging, statistical analysis, performance monitoring, improvements may include the following:

    3.1. 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;

    3.2. (ID Validate only) Customer reporting on prevalence of fake identity documents based and debugging of the fake classification.

4. Scandit will dispose of or anonymize the personal data transmitted to Scandit as part of the scan engine result from ID scanning products maximum 30 days after the scan. Scandit may retain anonymized data after this time period for product development purposes.