

ASSA ABLOY Terms and Conditions for Digital Solutions and Services

1. Connected solutions and services

To utilize data that is generated by ASSA ABLOY products owned by the customer ("**Customer**"), ASSA ABLOY provides digital solutions and services ("**Services**") to its customers. ASSA ABLOY shall provide the Services ordered by the Customer in accordance with these Terms and Conditions for Digital Solutions and Services ("**Agreement**"). The descriptions and details of the Services provided under this Agreement, is provided in a separate agreement entered into by ASSA ABLOY and the Customer ("**Main Agreement**").

Any natural or legal person who is authorized by ASSA ABLOY or the Customer to access the Services is referred to as a "**Service User**".

The Customer undertakes to ensure that any Service User appointed by the Customer agrees to adhere to the terms of this Agreement and its appendices.

2. Fees

The provision of the Services to the Customer by ASSA ABLOY under this Agreement is subject to Customer's timely payment of all fees owed to ASSA ABLOY or its authorized distributors or resellers transacting with the Customer for use of the Services, as provided in the Customer's order. All fees paid to ASSA ABLOY are non-refundable.

3. Data

The status, statistics, parameters, errors and event data which is generated by the products sold to the Customer or serviced by ASSA ABLOY will be used by ASSA ABLOY to provide, improve, and develop any ASSA ABLOY products or services, as the case may be. The data will be treated confidential.

4. Access and License

Subject to the Customer's timely payment of all fees owed hereunder, ASSA ABLOY grants to the Customer, in accordance with this Agreement, its appendices and the Main Agreement the right to access and use the Services during the term of this Agreement,

for Customer's own internal business operations and not for the benefit of any other person or entity. The license to access and use the Services is a personal, fully revocable, limited, non-transferable, non-exclusive, non-sublicensable license during the term of this Agreement to use the Services and the right to extend such license to the Service Users in object code form only and solely for the purpose of accessing the Services.

5. User obligations

The Customer and Service User shall use the Services in accordance with this Agreement and warrants that the Services or any element thereof will not be used for any purpose that is unlawful.

Customer and Service User warrants that it will keep Customer established passwords, temporary passwords provided by ASSA ABLOY, security credentials, or authentication keys provided or used in relation to the Services safe and secure and not disclose these for any unauthorized third party.

Customer and Service User shall not:

1. Re-sell, rent, lend, lease, distribute, or share the Services and any data or content within the Services (including on a "service bureau" basis), provide third parties with access or grant third parties rights to the Services or otherwise violate the license terms under Section 4 of this Agreement.
2. Alter or remove any marks or proprietary legends contained in the Services.
3. Interfere with or disrupt the integrity or performance of the Services.
4. Attempt to probe, scan, or test the vulnerability of the Services, software, system or network or breach any security or authentication measures, or to reverse engineer, decompile or otherwise attempt to access the source code of the Services.
5. Use the Services on any device that they do not own or control.
6. Solicit personal data for commercial or unlawful purposes.

7. Delete, change or modify in any way any copyright or patent notices or trademarks contained in the Services.
8. Use or launch any automated system, including without limitation, robots, spiders or other automatic device or manual process to monitor or copy the Services.
9. Provide to the Services any viruses, worms, time bombs, and/or other computer programming routines that are intended to damage, detrimentally interfere with, intercept or expropriate any system, data or information or any content that may create liability for ASSA ABLOY or cause ASSA ABLOY to lose (in whole or in part) the services of our suppliers.
10. Engage in any act that interferes with ASSA ABLOY's business or violates the license and right to use or infringes ASSA ABLOY's or any third party's intellectual property rights.

Any attempt by the Customer or Service User to engage in the aforementioned actions constitutes a violation of ASSA ABLOY's rights, as well as those of its licensors or distributors, and represents a material breach of this Agreement. The Customer shall hold ASSA ABLOY harmless for any damages suffered by ASSA ABLOY caused by Customer's or Service User's breach of this Section 5.

6. Misuse

If ASSA ABLOY determines that the Customer's or Service User's activity on the Services imposes an unreasonable load on bandwidth or infrastructure, ASSA ABLOY may at its sole discretion impose controls to keep the usage at reasonable levels.

Should ASSA ABLOY reasonably suspect or conclude that Customer or Service User is in breach of any part of this Agreement, ASSA ABLOY is entitled to immediately revoke access to the Services.

7. Data Protection

ASSA ABLOY will process personal data of the Customer and Service Users as a Data Controller when administering the provision of the Services under this Agreement in accordance with ASSA ABLOY's Privacy Notice found at <https://www.assaabloyentrance.com/master-blueprint/en/market->

[documents/products/digital-solutions/Insight%20Privacy%20Notice.pdf](#)

ASSA ABLOY will process personal data as a Data Processor on behalf of the Customer in accordance with the Data Processing Agreement found in Appendix 1 of this Agreement.

8. Obligations

ASSA ABLOY's provision of the Services is based on the requested Customer configurations. The Customer acknowledges and agrees that the Customer is solely responsible for the Customer configurations and assures that the selection conforms to the Customer's policies and procedures and complies with all applicable laws and regulations in jurisdictions in which the Customer accesses and uses the Services.

Customer represents and warrants that:

1. It will comply with all applicable privacy and data protection laws and regulations applicable to its business and its performance of its obligations under this Agreement with respect to any data uploaded to, submitted to, stored on, or processed by the Services;
2. It will provide any notices and obtain required consents related to its use of the Services and ASSA ABLOY's provision of the Services, including those related to the collection, use, transfer, monitoring, and disclosure of personal data; and
3. It shall prevent Service Users from using the Services in breach of this Agreement.

9. Confidentiality

Any information provided by ASSA ABLOY regarding the know-how, inventions (whether or not patentable), techniques or ideas, related to the Services; the design and architecture of the Services; the computer code, internal documentation, and design and functional specifications of the Services; the pricing of the Services provided directly from ASSA ABLOY; the terms of this Agreement; and any problem reports, analysis and performance information related to the Services shall be regarded as confidential.

10. Limitation of Liability

The Services are provided "as is", and ASSA ABLOY is entitled to make updates and changes to the Services from time to time. To the maximum extent permitted by applicable law, ASSA ABLOY disclaims all warranties whether express or implied, including but not

limited to implied warranties of merchantability, fitness for a particular purpose, warranties arising from course of dealing or course of performance, freedom from malicious code, of accuracy, title and non-infringement of third party rights, with regard to the Services. ASSA ABLOY does not warrant that the Services will meet the Customer's requirements, be uninterrupted, timely, error-free, secure or free of viruses, worms, disabling code or conditions or the like, or that the results that may be obtained from the use of the Services will be accurate or reliable.

ASSA ABLOY's aggregate liability under this Agreement shall be limited to the lower of i) the actual fees paid by the Customer for the Services during the last 12-month period or ii) one thousand (€1 000) EUR.

Notwithstanding any other provision in this Agreement, neither party shall be liable for any indirect, incidental, or consequential damages or loss or costs of procuring substitute goods, software, or services, even if it has been advised of the possibility of

such damages, arising out of or in connection with this agreement.

11. Miscellaneous

This Agreement shall hold precedence over the Main Agreement regarding the provision of the Services if contradictory. The Main Agreement shall be used for interpreting and supplementing this Agreement.

ASSA ABLOY may amend this Agreement from time to time publishing the updated version on the website <https://www.assaabloyentrance.com/global/en/solutions/products/digital-solutions>.

If any provision of this Agreement or the application of it shall be declared or deemed void, invalid or unenforceable in whole or in part for any reason, the parties shall amend this Agreement as shall be necessary to give effect to the spirit of this Agreement so far as possible. If the parties fail to amend this Agreement, the provision which is void, invalid or unenforceable, shall be deleted and the remaining provisions of this Agreement shall continue in full force and effect.

APPENDIX 1 - DATA PROCESSING AGREEMENT

1. Roles of the parties in relation to the processing of personal data

1.1 ASSA ABLOY will process personal data as a Data Processor on behalf of the Customer as Data Controller (jointly referred to as the “Parties”) in accordance with the Customers documented instructions as set out in this Data Processing Agreement (“DPA”). The processing activities ASSA ABLOY will carry out as Data Processor are described in Annex I of this DPA.

The terminology used in this DPA shall be interpreted in accordance with the definitions provided in Regulation (EU) 2016/679 (the General Data Protection Regulation or “GDPR”).

2. Sub-processing

2.1 The Parties agree that ASSA ABLOY has a general authorization from the Customer to engage Sub-Processors for carrying out specific processing activities. The current list of agreed Sub-Processors is provided in Annex I.

2.2 ASSA ABLOY shall inform Customer if a new Sub-Processor will be engaged to process personal data on behalf of the Customer at least 10 days prior to the start of the processing activities. If the Customer provides valid reasons for objecting to a new Sub-Processor within 30 days from the notification of the engagement of a new Sub-Processor, both Parties will collaborate to find a suitable solution. If the Parties do not reach a mutually acceptable solution within a reasonable time, ASSA ABLOY is entitled to terminate this DPA and the Agreement as well as the Main Agreement if the provision of the Services without the intended Sub-Processor is impossible or commercially unreasonable.

2.3 Information regarding a new Sub-Processor shall include the following information:

(i) the identity and address of the Sub-Processor,

(ii) the type(s) of service(s) provided by the Sub-Processor,

(iii) the location of processing, and

(iv) where information can be found regarding technical and organizational security measures implemented by the Sub-Processor.

2.4 Where the processing activities involve a transfer of personal data outside of the EU/EEA, ASSA ABLOY and such Sub-Processor shall implement necessary safeguards in accordance with the GDPR.

3. Notification of personal data breaches

3.1 The Parties agree that ASSA ABLOY shall notify Customer no later than 24 hours after becoming aware of a data breach, unless ASSA ABLOY can provide sufficient reasoning for a later notification. Breach notifications shall be made to the email address provided by the Customer.

4. Audits

4.1 The Customer has a right to request documentation regarding technical and organizational security measures from ASSA ABLOY once per year or to the extent required by applicable law, to ensure ASSA ABLOY’s compliance with this DPA.

4.2 The Parties agree that each Party will bear its own costs for audits. Should an audit or inspection show that ASSA ABLOY has not fulfilled its obligations under this DPA, ASSA ABLOY shall remedy such issue at its own cost.

5. Compliance with law

5.1 ASSA ABLOY shall have the right to request any necessary changes (including amendments) to the provisions of this DPA if necessary to comply with mandatory provisions of applicable data protection law.

5.2 ASSA ABLOY will offer reasonable support to the Customer in their efforts to comply with mandatory data protection laws. This includes assisting the Customer in ensuring compliance with the obligations laid

down in Articles 32-36 in the GDPR, considering the nature of the personal data processing and the information available to ASSA ABLOY.

6. Confidentiality

- 6.1 ASSA ABLOY shall ensure that those with access to the Customer's personal data, such as ASSA ABLOY employees and subcontractors, shall keep such personal data strictly confidential.

7. Data retention

- 7.1 ASSA ABLOY will only process the Customer's personal data during the term of the provision of the Services under the Agreement and the Main Agreement. ASSA ABLOY will, at the choice of the Customer, erase or return all personal data to the Customer after the end of the provision of the Services, and erase any existing copies of the personal data unless the retention of the personal data is required by union or member state law.

8. Miscellaneous

- 8.1 In the event of inconsistencies between the provisions of this DPA and any other agreement between the Parties in relation to the data protection obligations addressed herein, the provisions of this DPA shall prevail.
- 8.2 If any provision of this DPA should be held to be invalid or unenforceable, the remaining provisions shall remain in full force and effect. The invalid or unenforceable provision shall be deemed to be automatically replaced by a valid and enforceable provision that comes closest to the purpose of the invalid or unenforceable provision.
- 8.3 This DPA inures to the benefit of the Parties only and no third party shall have any rights hereunder, except as expressly stated otherwise in this DPA.
- 8.4 This DPA replaces any previous data protection related agreement(s).

ANNEX I – DATA PROCESSING ACTIVITIES

1. Description of the processing of personal data

For the provision of the Services, ASSA ABLOY will carry out the following processing activities:

<i>Processing Activity</i>	<i>Categories of data subjects</i>	<i>Categories of personal data</i>	<i>Storage period</i>	<i>Sub-Processors</i>
Access administration	<ul style="list-style-type: none">• Customers• Service Users	<ul style="list-style-type: none">• Name• Email address	Service term	<ul style="list-style-type: none">• Auth0 Inc.• Amazon Web Services Inc.
Notification send-outs	<ul style="list-style-type: none">• Customers• Service Users	<ul style="list-style-type: none">• Name• Email address	Service term	<ul style="list-style-type: none">• Amazon Web Services Inc.

Place of processing

Personal data is processed by ASSA ABLOY and its Sub-Processors in the EU.

Frequency of the processing and transfers

During the term of the Agreement.

2. Technical and Organizational Security Measures

ASSA ABLOY shall take the technical and organizational security measures that are necessary under Article 32 in the GDPR. The following technical and organizational security measures have been implemented by ASSA ABLOY to protect the Personal Data covered by this DPA:

- **Access Control:** Implementation of robust access management protocols, including password management, multi-factor authentication (MFA), logging, user roles and permissions, and secure access to cloud resources and operational environments.
- **Confidentiality Measures:** Data is protected through end-to-end encryption, both in transit and at rest, to ensure the confidentiality of customer data across cloud infrastructure.
- **Availability Measures:** High availability is maintained through automated backups, distributed firewall protection, advanced antivirus systems, comprehensive logging, and scalable cloud architecture with failover capabilities and redundancy to ensure minimal downtime.

3. List of Sub-Processors

<i>Name</i>	<i>Contact details</i>	<i>Place of processing</i>	<i>Description of processing</i>
Auth0 Inc.	dpa@okta.com	EU	Access administration
Amazon Web Services Inc.	aws-notification-intake@amazon.com	EU	Access administration Notification send-outs