

## Privacy Notice - ASSA ABLOY Digital Solutions and Services

We, ASSA ABLOY Entrance Systems AB, Reg. No. 556204-8511, ("**ASSA ABLOY**") are committed to protect your personal data. All processing of personal data takes place in accordance with current data protection legislation.

This Privacy Notice describes how we collect and process the personal data that we receive about you when you are granted access and use digital solutions and services provided by ASSA ABLOY under the [ASSA ABLOY Terms and Conditions for Digital Solutions and Services](#) ("**Services**"). This notice also describes how you can contact us if you have additional questions regarding our processing of your personal data.

To find more details regarding the Services, please visit [ASSA ABLOY Terms and Conditions for Digital Solutions and Services](#) [<https://www.assaabloyentrance.com/global/en/solutions/products/digital-solutions>]

If you are an employee or consultant working for us, then please also see the [Privacy Notices for Employees and Consultants](#) that have been provided to you during your onboarding process and that are also available on our [Intranet](#).

## Privacy Notice Contents

Click here for:

- [Detailed Descriptions of Processing Activities.](#)
- [More information on your rights under the GDPR.](#)
- [How to contact us if you have questions or want to exercise your rights under the GDPR.](#)
- [How to contact your Supervisory Authority.](#)
- [List of recipients of Personal Data transfers.](#)
- [List of Personal Data categories used in this Privacy Notice.](#)

## Summary of situations where we will process your Personal Data

We will process Personal Data belonging to you in the following situations:

- [ACCESS MANAGEMENT](#)
- [NOTIFICATIONS AND REPORTS](#)
- [TECHNICAL LOGS](#)

## Detailed Descriptions of Processing Activities

### ACCESS MANAGEMENT

<b>Purpose</b>	To ensure that only the persons permitted to use the Services are provided access, we will process personal data to administrate the access to the Service.
<b>Personal Data Categories</b>	<ul style="list-style-type: none"> <li>• Email address</li> <li>• Name</li> <li>• Unique identifier</li> <li>• IP address</li> <li>• Password</li> </ul>
<b>Personal Data Sources</b>	<p>Your email address and name are either provided to ASSA ABLOY by you directly, or by the administrator that gives you access to the Services, when you are given access to the Services. The administrator can either be ASSA ABLOY or a customer of ASSA ABLOY.</p> <p>The unique identifier is created and assigned to you when you are given access to the Services.</p> <p>Your IP address will be collected when you access the service and stored to relate to your unique identifier.</p>
<b>Legal Ground</b>	<p>Legitimate Interest (GDPR Article 6.1.f).</p> <p>Our legitimate interest for processing your personal data is to provide access to the ASSA ABLOY Digital Solutions and Services requested either by you or by an administrator assigning you access to the Service on your behalf. Also, our interest is to ensure that only authorized access is permitted.</p>
<b>Retention</b>	Your personal data will be kept as long as you have access to the Service.
<b>Transfers</b>	<p>To our <a href="#">Access Management Service Provider</a> in their capacity as Processor acting on our behalf.</p> <p>To our <a href="#">Data Centre Service Provider</a> in their capacity as Processor acting on our behalf.</p>

## NOTIFICATIONS AND REPORTS

<b>Purpose</b>	The purpose of sending out notifications and reports via email, push notifications on your smart phone and in the Services is to ensure that you receive information regarding errors and events in the Service and to provide you the possibility to view and use reports in and outside the Service.
<b>Personal Data Categories</b>	<ul style="list-style-type: none"> <li>Email address</li> </ul>
<b>Personal Data Sources</b>	Your email address is used to send out reports to your email and to notify you in the Services. Your email address is either provided to ASSA ABLOY by you directly, or by the administrator that gives you access to the Services, when you are given access to the Services. The administrator can either be ASSA ABLOY or a customer of ASSA ABLOY.
<b>Legal Ground</b>	<p>Legitimate Interest (GDPR Article 6.1.f).</p> <p>Our legitimate interest is to send you emails and notifications regarding events and reports regarding the Service.</p> <p>The reports are only sent out if you choose to subscribe to the reports, and you can unsubscribe at any time through the Services. The push notifications are only sent to you if you have enabled push notifications for the Insight Mobile application in your smart phone, and you can switch off the push notifications at any time through the settings on your smart phone.</p>
<b>Retention</b>	N/A
<b>Transfers</b>	To our <a href="#">Data Centre Service Provider</a> in their capacity as Processor acting on our behalf.

TECHNICAL LOGS

<p><b>Purpose</b></p>	<p>We keep technical logs containing information regarding your actions in the Service, including technical information, to ensure that the Service is functioning properly, and for troubleshooting if any errors would occur. We may also use the technical logs to investigate any suspicion of misuse of the Service.</p>
<p><b>Personal Data Categories</b></p>	<ul style="list-style-type: none"> <li>• Email address</li> <li>• Name</li> <li>• Unique identifier</li> <li>• IP address</li> <li>• Actions taken in the Service</li> </ul>
<p><b>Personal Data Sources</b></p>	<p>The personal data is collected from your use of the Service and the personal data stored for the access management.</p>
<p><b>Legal Ground</b></p>	<p>Legitimate Interest (GDPR Article 6.1.f). Our legitimate interest is to ensure that the Service is functioning properly and that we can correct any errors swiftly. Our interest is also to ensure that the Service is not misused.</p>
<p><b>Retention</b></p>	<p>The technical logs are kept for 30 days.</p>
<p><b>Transfers</b></p>	<p>To our <a href="#">Access Management Service Provider</a> in their capacity as Processor acting on our behalf. To our <a href="#">Data Centre Service Provider</a> in their capacity as Processor acting on our behalf.</p>

## Your Rights According to the GDPR

You have the following rights according to the GDPR.

If you wish to exercise these rights, then please contact us using the contact information provided in the next section.

We normally respond to your request within one month following the date we received your request. However, if your request is complicated or if you have submitted several requests, we may need additional time to handle your request. We will in such a case notify you and the reasons of the delay. If we cannot, wholly or in part, comply with your request we will notify you and the reasons for this.

Description of Right	When and how the Right Applies
<p><b>Withdrawal of consent (Article 7.3 of the GDPR):</b></p> <p>You have the right to withdraw any consent given to us allowing us to use your personal data in a specific way. If you choose to withdraw such a consent, we shall immediately cease the related use of your personal data and delete or anonymise the associated personal data immediately.</p>	<p>This will only apply to those uses of your personal data that are based on you having given us consent for that use. If we rely on other legal bases than consent for the use of your personal data, then withdrawing a consent will not affect those uses. Please see each relevant section regarding our use of personal data for information on which legal bases we rely on in each situation and thus which use of your personal data that is based on your consent.</p>
<p><b>Right of access (Article 15 of the GDPR):</b></p> <p>You have the right to obtain confirmation from us as to whether we are processing personal data about you, and, where that is the case, access to a copy of the personal data together with information about our use of your personal data.</p>	<p>Please note that the right to a copy of your personal data may not adversely affect the rights of others. This means that the information that can be accessed is restricted to personal data belonging to you. Business information or personal data belonging to other individuals will not be included in an access request response.</p>

**Description of Right****When and how the Right Applies****Right to rectification (Article 16 of the GDPR):**

You have the right to obtain without undue delay the rectification of inaccurate personal data about you. Considering the purposes of the processing, you have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

Please note that historical information may not necessarily be incorrect, meaning that the right to rectification may not in a specific case apply to such historical information. This depends on the purposes of the use of the personal data.

**Right to erasure (Article 17 of the GDPR):**

You have in certain situations the right to request erasure or deletion of your personal data ("the right to be forgotten").

The right to erasure will only apply in certain situations. For example, the right to erasure applies where we do not have a valid justification for retaining and continuing to use the personal data. This will typically be cases where we have failed to delete personal data after you have withdrawn your consent or when we have failed to observe the retention period of personal data. It may also be a case where you have successfully objected to our use of personal data and we cannot show a compelling reason to continue using your personal data despite your objection. There are also several exemptions from the right to erasure, including if we are obligated under law to keep your personal data or if the personal data is needed to exercise, manage, and defend legal claims.

## Description of Right

## When and how the Right Applies

### **Right to restriction (Article 18 of the GDPR):**

You have in certain situations the right to request that the use of your personal data is restricted, which means that you can, at least for a certain period, stop us from using your personal data in other ways than just storing your personal data.

The right to restriction of the use of your personal data will only apply in certain situations. The right to restriction applies if you have objected to our use or if you consider that your personal data is incorrect or incomplete and during the period that we manage your objection or verify whether the personal data is incorrect or incomplete. The right to restriction also applies if we no longer need the personal data for the purposes that we collected the personal data, but you need the personal data to manage, defend or exercise legal claims and rights. In such a case we will continue to store your personal data for as long as you need the personal data for this purpose.

If the use of your personal data has been restricted, we may normally only store your personal data and not use them for any other purpose than to manage, defend or exercise legal claims and rights. We can also use your personal data for other purposes if you have given your consent to such use.

### **Right to data portability (Article 20 of the GDPR):**

You have the right to a copy of certain personal data about you in a structured, commonly used and machine-readable format and, if it is technically feasible, the right to request that the copy of your personal data is transferred directly to an external recipient.

The right to data portability only applies to personal data that we have collected, and use based on your consent (Article 6.1 (a) of the GDPR) or in order to fulfil an agreement with you (Article 6.1 (b) of the GDPR). Moreover, the right is limited to personal data that you yourself has provided to us.

Please see each relevant section regarding our use of personal data for information on which legal bases we rely on in each situation.



## Description of Right

## When and how the Right Applies

### **Right to object (Article 21 of the GDPR):**

In certain situations, you have the right to object to our use of your personal data. Where the right to object applies, this means that we must stop using your personal data in the specific situation.

The right to object applies under specific circumstances. You always have the right to object to our use of your personal data for direct marketing purposes. In marketing communications, we always include an opt-out link that you can use to unsubscribe to such communications.

Moreover, where we rely on a legitimate interest for the use of your personal data, you have the right to object to the use for reasons which relates to your particular situation. If we in such a situation cannot show a compelling reason to continue to use your personal data, we will stop using your personal data for the relevant purpose.

Please note that the right to object does not apply if the personal data is needed to exercise, manage, and defend legal claims.

### **Right to object to automated individuation decision-making (Article 22 of the GDPR):**

You have the right to object to decisions based solely on automated processing, including profiling, which produces legal effects concerning you or which similarly significantly affects you.

This means that if we have made a decision that will significantly affect you or which produces legal effects, and that decision was made automatically, you have the right to object to the automated decision and request a manual review of the decision.

## How to Contact Us

If you have questions, complaints or want to exercise your rights according to the GDPR then please use one of the proposed channels below to contact us.

When you write to us, please provide information about the relationship that you have or have had with ASSA ABLOY including the nature of the relationship and the subsidiary/subsidiaries that you have had that relationship with. This will help us respond to your question or request.

We will in most cases need to verify your identity. This is a legal obligation which we must adhere to. When verifying your identity, we may need to request additional information from you. We only request the information that is necessary to verify your identity in the specific situation.

### Data Protection Officer:

ASSA ABLOY has as a general rule not appointed and registered a Data Protection Officer according to GDPR Article 37. Some countries however have local requirements making it mandatory for ASSA ABLOY to register a Data Protection Officer for those countries. Below is a list of those countries where ASSA ABLOY has appointed a Data Protection Officer together with the contact information to the registered Data Protection Officer.

Country	Data Protection Officer	Contact Information
DE	Wolfgang Steger	Am Neuen Weg 21 82041 Oberhaching DEUTSCHLAND

### Physical Letter:

ASSA ABLOY Entrance Systems AB  
Attention: ESD Data Protection Manager  
Lodjursgatan 10  
261 44 Landskrona  
SWEDEN

*We would appreciate that you write a physical letter in English if possible. This will help us handle your request. This is however not a requirement.*

**E-mail:**

Please select the e-mail address in the table below that corresponds to the country where you reside, alternatively where the ASSA ABLOY Entrance Systems entity you have been in contact with is based.

<b>Country</b>	<b>E-mail Address</b>
AT	privacy.at.entrance@assaabloy.com
BE	privacy.be.entrance@assaabloy.com
CH	privacy.ch.entrance@assaabloy.com
CZ	privacy.cz.entrance@assaabloy.com
DE	privacy.de.entrance@assaabloy.com
DK	privacy.dk.entrance@assaabloy.com
ES	privacy.es.entrance@assaabloy.com
FI	privacy.fi.entrance@assaabloy.com
FR	privacy.fr.entrance@assaabloy.com
HU	privacy.hu.entrance@assaabloy.com
IE	privacy.ie.entrance@assaabloy.com
IT	privacy.it.entrance@assaabloy.com
NL	privacy.nl.entrance@assaabloy.com
NO	privacy.no.entrance@assaabloy.com
PL	privacy.pl.entrance@assaabloy.com
PT	privacy.pt.entrance@assaabloy.com
RO	privacy.ro.entrance@assaabloy.com
SE	privacy.se.entrance@assaabloy.com

<b>Country</b>	<b>E-mail Address</b>
SI	privacy.si.entrance@assaabloy.com
TR	privacy.tr.entrance@assaabloy.com
UK	privacy.uk.entrance@assaabloy.com

## Your Supervisory Authority

Each EU/EEA member state shall have its own supervisory authority for data protection. You have the right to contact or lodge a complaint with the supervisory authority in your country.

To ensure that we provide you with the latest and correct information about the supervisory authority in your country, we ask you to follow the link below to the official list of supervisory authorities. If you are in doubt, contact us using the channels above and we will help you find your local supervisory authority.

Link to the EDPB list of current supervisory authorities: [https://edpb.europa.eu/about-edpb/board/members\\_en](https://edpb.europa.eu/about-edpb/board/members_en)

Given that ASSA ABLOY is a Swedish legal entity, the supervisory authority that supervises our use of personal data is the Swedish data protection authority, the Swedish Authority for Privacy Protection (IMY) <https://www.imy.se/>.

## Recipients of Personal Data transfers

The list below contains descriptions of the Recipient labels that have been used in the descriptions of our use of your Personal Data:

Recipient Label	Recipient Name	Recipient Country
Access Management Service Provider	Auth0 Inc.	EU
Data Centre Service Provider	Amazon Web Services Inc.	EU