

APICA PRIVACY POLICY

Last Updated: November 3, 2021

1. INTRODUCTION

Apica, a Swedish corporation with headquarters at Malmkillnadsgatan 32, 111 51, Stockholm, Sweden (hereafter 'Apica', 'we' or 'us') is committed to protect your personal data and to respect your privacy.

The General Data Protection Regulation (GDPR) is a European privacy law that became enforceable on May 25, 2018. The GDPR replaced the EU Data Protection Directive, also known as [Directive 95/46/EC](#), and intended to harmonize data protection laws throughout the European Union (EU) by applying a single data protection law that is binding throughout each member state.

This privacy policy ('Privacy Policy') explains the reason for the processing of your personal data, the way we collect, handle and ensure protection of all personal data from or about you as a private individual, how that information is used and what rights you have in relation to your personal data. It also specifies the contact details of the responsible 'Data Controller' with whom you may exercise your rights and the 'Integritetsskyddsmyndigheten' ('Swedish Authority for Privacy Protection').

The information in relation to processing operation on Apica SaaS services, Apica Synthetic Monitoring (hereafter 'ASM'), Apica LoadTest (hereafter 'ALT'), and the Apica publicly available website apica.io (hereafter 'ApicaWeb'), is presented below.

If you have questions or complaints regarding this Privacy Policy, or regarding your personal data relating to the Apica SaaS services, ASM, ALT and the ApicaWeb, please write to us at support@apicasystems.com

2. WHY AND HOW DO WE COLLECT AND PROCESS YOUR PERSONAL DATA?

The collecting and processing of your personal data is for the purpose of providing (administratively and electronically) and supporting (such as keeping statistics, optimizing, uphold safety and security, and to comply with legal requirements), the Apica SaaS services ASM, ALT and the ApicaWeb. These services are designed to be used for monitoring, loadtesting and information publications for individuals, corporations, organization or other.

Apica collects and uses your personal information to manage user populations and their rights in the context of IT systems. The main purpose of this is to ensure the appropriate level of security is applied in a consistent fashion across Apica IT services with the ability to identify the user of the service, authenticate that user, and / or determine his or her authorisations and roles within the context of their service. The ASM and ALT services allow authentication of individuals (hereafter 'PortalUsers') that are representatives of corporations, organization or other entity that have entered into a contractual agreement with Apica.

The ApicaWeb does not require authentication and is publicly available and any ApicaWeb users (hereafter 'ApicaWeb individuals') may self-register (hereafter 'ApicaWeb self-registered individuals') if they want more information about Apica products etc.

Additional purposes for this processing operation, are the following:

- Services, allowing individuals contact details to be found (e.g. e-mail address book or telephone directory)
- Selection of individuals from lists, usually based on some selection criteria
- Construction of lists of individuals, primarily e-mail distribution lists
- Customization of user interfaces according to users' individual characteristics

The processing is automated and performed by means of computer/machine.

Your personal data will not be used for an automated decision-making including profiling.

Integrations with different SaaS services from ASM and ALT that rely on commonly required personal data, may nevertheless collect additional personal data themselves. This data processing will be covered by the services' own privacy statements usually available on their respective web pages.

3. ON WHAT LEGAL BASIS DO WE PROCESS YOUR PERSONAL DATA

We process your personal data in our SaaS services ASM and ALT, because:

Art. 6 GDPR

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

The personal data of the PortalUsers is processed **based on the contractual agreement**, that includes the Apica General Terms and Conditions and the Apica Data Processing Agreement.

We process your personal data on the ApicaWeb, because:

Art. 6 GDPR

(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

The personal data of the individuals visiting the ApicaWeb is processed based **on consent** after having read, understood and agreed to this Privacy Policy. Consent can be withdrawn at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Please note that if you request that Apica restricts or erases your personal data or if you withdraw your consent, this may lead to that the services no longer can be fully provided to you.

Apica also base its processing of your personal data on Apica's legitimate interest to provide **necessary functionality** required during use of the services, to do technical enhancements and for improving the standard of the services and security, to prevent misuse and illegal action, to collect statistics for the services, and to perform necessary log/register maintenance.

4. WHICH PERSONAL DATA DO WE COLLECT AND FURTHER PROCESS?

In order to carry out this processing operation Apica collects the following categories of personal data:

For PortalUsers, Apica is processing identification data (to identify the individuals):

- Personal information:
 - First and last name(s) as provided in the contracts,
 - Email
 - Phone
 - Mobile
 - Organizational number / ID
 - Street address
 - P.O. box
 - Zip code
 - City
 - Country
 - Admin phone
 - Admin mobile
 - Admin email
 - Tech phone
 - Tech email
 - Custom reporting email
 - Time zone
 - Geographical region

Based on the above, ASM and ALT generates a unique:

- Customer id (based on specific rules)
- User id (based on specific rules)
- Username (based on specific rules)
- Password (based on specific rules)
- Customer api key (based on specific rules)
- User api key (based on specific rules)

ASM and ALT keeps a history of:

- Name changes (not to create multiple identities for the same individual)
- Password changes (to enforce regular changes (passwords are irreversibly encrypted))
- Last authentication and authenticated account activity (Date and time of the most recent successful and unsuccessful authentication and number of good logins and failed attempts)

This additional information is used to diagnose and resolve problems and to deal with security incidents as well as to avoid duplicated accounts. This information can help in following up any doubtful/malicious activity relating to your user account.

- Administrative data (to identify the relationship with the organization):
 - The corporation or organization or other entity of the individual

Based on the above Apica generates:

- Access rights - information about group membership (for granting access to the intended systems)

Please note that if you choose to integrate with a Single Sign On (SSO) provider in the ASM and ALT, we recommend you also read the privacy statements/notices of the related SSO integration service, since they are also applicable.

Log files for PortalUsers:

Each time the user logs in to the ASM and ALT portal protected by Login, the identifier, the site and the time will be recorded in a log file. The exact time of log-out will also be recorded for security purposes.

The provision of personal data is mandatory to meet access requirement for PortalUsers at Apica. If you do not provide your personal data, the consequence is that you will not be able to get access to the ASM and ALT systems.

We have obtained your personal data either from the corporation or organization or other entity, or directly from the data subject for the self-registered individuals.

For ApicaWeb self-registered individuals, Apica is processing identification data:

- Personal information (as provided by the individual during self-registration):
 - first and last name(s)
 - e-mail address
 - mobile number
 - country
 - product interested in

Anonymous usage statistics:

Apica may also collect anonymous usage statistics to be used solely by Apica to improve the Apica services and to find and fix problems and for improving safety and security when using the services.

Other:

As for most websites and services delivered over the Internet, Apica gathers certain information and stores it in log files when you interact with our websites and services (also see section '10. HOW APICA USES COOKIES' below). This information includes internet protocol (IP) addresses as well as browser type, internet service provider, URLs of referring/exit pages, operating system, date/time stamp, information you search for, locale and language preferences, identification numbers associated with your devices, and system configuration information. Occasionally, Apica connects personal data to information gathered in our log files as necessary to improve our Websites and the services. In such a case, we will treat the combined information in accordance with this Privacy Policy.

Location data and biometric data:

Apica and the services do not take part in any collection, processing, or storage of specific location data (except geographical region) and biometric data, such as Face-ID, fingerprint, voice recognition. Each provider of these services is responsible for such data, through its services and operating systems.

5. HOW LONG DO WE KEEP YOUR PERSONAL DATA?

In general, Apica only keeps your personal data for the time necessary to fulfil the purpose of collection or as needed to perform our contractual obligations to you, to provide the services, to comply with legal obligations, to resolve disputes, to preserve legal rights, or to enforce our agreements.



Data and files related to the ASM and ALT PortalUsers are kept as long as the the corporation or organization or other entity has a contractual agreement with Apica and up to 180 days after termination of such contractual agreement.

Log files related to the ASM, and ALT services are not kept for any longer than is necessary in light of the reason(s) for which it was first collected.

Data and log files related to ApicaWeb self-registered individuals are not kept for any longer than is necessary in light of the reason(s) for which it was first collected.

Please note that your personal data may be retained longer for reasons described in section 7 ('7. WHO HAS ACCESS TO YOUR PERSONAL DATA AND TO WHOM IS IT DISCLOSED?'), but then such data will be kept in an aggregated and anonymized way.

6. HOW DO WE PROTECT AND SAFEGUARD YOUR PERSONAL DATA?

In order to protect your personal data, Apica follows generally accepted standards to protect the personal data submitted to us, both during transmission and once it is received and stored . These security and privacy practices include appropriate actions to address online security, risk of data loss, alteration of data or unauthorised access, taking into consideration the risk presented by the processing and the nature of the personal data being processed. Organisational measures include restricting access to the personal data solely to authorised persons with a legitimate need to know for the purposes of this processing operation. Apica's security and privacy practices are found in Apica's applicable data security standards at apica.io/dpa.

All personal data collected by Apica regarding our ASM, ALT customers and PortalUsers, are stored and processed on servers owned by Apica. Apica are currently using its own servers in datacenters hosted by GlobalConnect and Amazon Web Services for data processing and data storage (IaaS) for Apica SaaS services ASM and ALT, with servers in Sweden, United Kingdom, Germany, Ireland, and USA. However processing and storage procedures may include that collected data and/or personal data may be transferred outside of these regions/countries and when required for integrations stored and processed by external third parties, acting as processor[-s] of Apica, that are based both inside and outside of the European Economic Area (EEA).

All personal data collected by Apica regarding the ApicaWeb visitors and ApicaWeb self-registered individuals are stored and processed on services contracted by Apica and hosted by external third parties such as WP Engine and HubSpot with servers in Germany and USA. However processing and storage procedures may include that collected data and/or personal data may be transferred outside of these regions/countries and when required for integrations stored and processed by external third parties, acting as processor[-s] of Apica, that are based both inside and outside of the European Economic Area (EEA).

Having Apica's ASM and ALT services infrastructure for its operation with GlobalConnect and Amazon Web Services, and Apica's ApicaWeb services for its operation with WP Engine and HubSpot provides security that is designed and managed in alignment with best security practices and a variety of IT security standards and certified under several global compliance programmes which underlines best practices in terms of data centre security.

All personal data Apica collects which is stored and processed in our own servers hosted by GlobalConnect and Amazon Web Services, and services provided by WP Engine and HubSpot can only be accessed by Apica.

All communication and transfer of personal data to and from Apica to our own servers hosted by GlobalConnect and Amazon Web Services, and services provided by WP Engine and HubSpot is encrypted. We use best practices in terms of encryption and security.

For more information about Amazon Web Services, WP Engine and HubSpot managed services for transfer of personal data and reasons for why they may share personal data please refer to their specific privacy policies and data processing agreements at:

Amazon Web Services aws.amazon.com/compliance/data-protection/

WP Engine wpengine.com/legal/

HubSpot legal.hubspot.com/security

7. WHO HAS ACCESS TO YOUR PERSONAL DATA AND TO WHOM IS IT DISCLOSED?

Access to your personal data is provided to Apica staff responsible for carrying out this processing operation and to authorised staff according to the 'need to know' principle. Such staff abide by statutory and confidentiality agreements.

Apica also only shares your personal data third-party service providers that Apica uses to provide hosting for and maintenance of Apica services, backup, storage, payment processing, analytics, and other services for Apica. These third-party service providers may have access to or process your personal data for the purpose of providing services to Apica.

Apica does not permit any third-party to use your personal data for marketing purposes or for any other purpose than in connection with the services they provide to Apica.

In certain situations, Apica may be required to disclose your personal data in response to lawful requests by public authorities, including to meet national security or law enforcement requirements. Apica may disclose such data to respond to subpoenas, court orders, or legal process, or to establish or exercise our legal rights or defend against legal claims. Apica may also share

such information to the extent necessary to investigate, prevent, or act regarding illegal activities, suspected fraud, situations involving potential threats to the physical safety of any person, violations of our applicable subscription/license agreements, or as otherwise required by law.

Apica may also share personal data with other third parties when we have your consent to do so.

8. WHAT ARE YOUR RIGHTS AND HOW CAN YOU EXERCISE THEM?

You have specific rights as a 'data subject' under GDPR, in particular the right to access your personal data and to rectify them in case your personal data are inaccurate or incomplete. Where applicable, you have the right to erase your personal data, to restrict the processing of your personal data, to object to the processing, and the right to data portability.

You have the right to object to the processing of your personal data, which is lawfully carried out pursuant to Article 5 (1) on grounds relating to your particular situation.

Please note that if you request that Apica restricts or erases your personal data or if you withdraw your consent, this may lead to that the services no longer can be fully provided to you.

For ApicaWeb individuals and ApicaWeb self-registered individuals:

You may restrict our use of Cookies. For more information, see '10. HOW APICA USES COOKIES'.

You have consented to provide your personal data to Apica for the present processing operation. You can withdraw your consent at any time by notifying Apica. The withdrawal will not affect the lawfulness of the processing carried out before you have withdrawn the consent.

You can exercise your rights by contacting "The Data Controller" as specified under '9. CONTACT INFORMATION'.

If necessary, you can also address "Integritetsskyddsmyndigheten". Their contact information is also given under "9. CONTACT INFORMATION".

Where you wish to exercise your rights in the context of one or several specific processing operations, please provide their description in your request.

9. CONTACT INFORMATION

- The Data Controller

If you would like to exercise your rights under GDPR, or if you have comments, questions or concerns, or if you would like to submit a complaint regarding the collection and use of your personal data, please feel free to contact:

- For ASM and ALT PortalUsers, your Apica sales representative.
- For ApicaWeb individuals by email to: support@apicasystems.com

- Integritetsskyddsmyndigheten

By email to: imy@imy.se or by visiting their website www.imy.se

10. HOW APICA USES COOKIES

Cookies are small text files that can be used by sites and services to make a user's experience more efficient and to help you access site and services faster and more efficiently. When you visit a site or service that uses Cookies for the first time, one is downloaded onto your computer or device. Sites and services may also use a similar technology called a Web beacon which is also known as pixel or clear GIF technology. When you next visit the site, your computer or device checks to see if it has a cookie from that site or service and sends the information from the Cookie to the site or service, and thus then 'knows' that you have been there before. Cookies, Web beacons, pixels and similar technologies used to remember you may expire when your session is closed to the site or service as when you close your browser, and some may last for longer. You can choose to delete Cookies on your computer or device at any time, however you may lose any information including, but not limited to, login and personalization settings. You can also choose to enable or disable Cookies in your internet browser. Most internet browsers also enable you to choose whether you wish to disable all Cookies or only third-party Cookies. By default, most internet browsers accept Cookies, but this can usually be changed. For further details, please consult the help menu in your internet browser or the documentation that came with your computer or device. It is recommended that you keep your internet browser and operating system up-to-date and that you consult the help and guidance provided by the developer of your internet browser and manufacturer of your computer or device if you are unsure about adjusting your privacy settings.

For ApicaWeb individuals, before Cookies are placed on your computer or device you will be shown a warning message requesting your consent to set those Cookies. By giving your consent to the placing of Cookies you are enabling us to provide the best possible experience and service to you. You may, if you wish, deny consent to the placing of Cookies from the ApicaWeb; however certain features of the ApicaWeb may not function fully or as intended.



Apica uses Cookies, Web beacons and other similar technologies for our site and services to:

- Identifying you when you use and/or sign in to the Apica ASM, ALT and ApicaWeb to provide you with recommendations, display personalized content, and provide other customized features and services.
- Remembering your specified configuration preferences and keeping track of them.
- Improve our services by diagnostics and conducting research.
- Improve security and to restrict and prevent fraud and fraudulent activity.
- To deliver content relevant to your interest, including ads.
- Perform reporting to measure and analyze performance of our site and services.

The information Apica collects through Cookies, Web beacons and other similar technologies for our site and services are:

- Your device or computer information, such as device type, application, or browser type and version, browser plug-in type and version, operating system, or time zone setting.
- The geographical location of your device or computer.
- Security related information such as authentication and security credentials for our site and services.
- Content interaction information such as content downloads, streams, and playback details, including duration and number of simultaneous streams and downloads.
- Network and connection information, such as information about your Internet service provider and the Internet Protocol (IP) address used to connect your device or computer to the Internet.
- Content you have viewed or searched for, page response times, download errors.
- Page interaction information such as scrolling, clicks, and mouse-overs.
- The full Uniform Resource Locators (URL) clickstream to, through and from our site and services including date and time.

You do not have to allow Apica to use these Cookies, however whilst Apica’s use of them does not pose any risk to your privacy or your safe use of the Apica site and services, it does enable Apica to continually improve them, making it a better and more useful experience for you.

By using Apica ASM and ALT services, and the ApicaWeb, you may also receive certain approved third parties third-party Cookies on your computer or device. Third-party Cookies are those placed by websites, services, and/or parties other than us. Third parties include providers of measurement and analytics services, search engines, social media networks and advertising companies. The Cookies are used to deliver content, save custom preferences, and measure the effectiveness of services and ads. To learn more about how these third parties use the information collected please review their privacy policies on their sites stated below.

Entity	Website
Amazon Web Services	https://aws.amazon.com/
Google	https://policies.google.com/
Microsoft	https://privacy.microsoft.com/
WP Engine	https://wpengine.com/
HubSpot	https://legal.hubspot.com/
PagerDuty	https://www.pagerduty.com/
Atlassian OpsGenie	https://www.atlassian.com/
ServiceNow	https://www.servicenow.com/
Slack	https://slack.com/
Splunk	https://www.splunk.com/
Cellsynt	https://www.cellsynt.com/
Pixie Data	https://www.pixie.se/
AppDynamics	https://www.appdynamics.com/
New Relic	https://newrelic.com/
Akamai Technologies	https://www.akamai.com/
Instana	https://www.instana.com/
Zendesk	https://www.zendesk.com/
Github	https://docs.github.com/
Sentry	https://sentry.io/
Hotjar	https://www.hotjar.com/

11. WHERE TO FIND MORE DETAILED INFORMATION

To contact Apica about anything that has to do with your personal data and data protection, including to making a subject access request, please use the following details:

Email address: support@apicasystems.com



Telephone numbers:

North America: +1 (310) 776-7569

EMEA: +46 8 4037-5000

12. CHANGES TO THIS PRIVACY POLICY

Should European Parliament and/or the Council pass new regulations and/or issue any guidelines, and any national laws adopted pertaining such changes, which contains terms that conflict with those used in this Privacy Policy, Apica reserves the right to change this Privacy Policy from time to time to make it compliant with any such new legislation or guideline.

Apica may change this Privacy Notice from time to time. This may be necessary, for example, if the law changes, or if Apica changes the business in a way that affects personal data protection.

Any changes of this Privacy Policy will be immediately posted on the ApicaWeb apica.io/privacy

We recommend that you check this page regularly to keep up to date.