

Data Processing Agreement

According to the EU General Data Protection Regulation (GDPR)

Version 1.4.2 of This Agreement was created on October 10, 2022.

This Data Processing Agreement (this “DPA”), effective as of the DPA Effective Date (defined below), is entered into by and between **Apaleo GmbH** (“Apaleo”, “we”, or “us”, “Processor”) and the **customer** that accepts or otherwise agrees or opts-in to this DPA (“Customer”, or “you”).

1 Introduction, area of application, definitions

- (1) This DPA stipulates the rights and obligations of the Customer and Apaleo (henceforth referred to as the ‘Parties’) in the context of processing personal data on behalf of the Customer.
- (2) This contract applies to all activities for which Apaleo’s employees or any subcontractors tasked with processing the Customer’s personal data.
- (3) The terms used in this DPA have the meaning given in the EU General Data Protection Regulation (GDPR).
- (4) “The Service” means the provisioning of property management software and related solutions as described on www.Apaleo.com
- (5) “Customer Data” means data you submit to, store on, or send to us via the Service.
- (6) “Subcontractor” means a third party that we use to process Customer Data to provide parts of the Service or related technical support. Additional services, such as transportation, maintenance and cleaning, as well as using telecommunication services or user services, do not apply.
- (7) “Data Breach” means a breach of Apaleo’s security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to Personal Data.
- (8) “in writing”, means the written form, as prescribed by § 126 BGB (Bürgerliches Gesetzbuch [*German Civil Code*]), or in another form under the condition that suitable verification is ensured.
- (9) “Master Contract” means the subscription and the PCI signed with Apaleo.
- (10) “Standard Contractual Clauses” or “SCCs” mean the standard contractual clauses as approved by the European Commission pursuant to its decision 2021/914 of 4 June 2021.

2 Scope and duration of the data processing

2.1 Scope

Apaleo is processing Customer data to provide services for property management, as described on www.Apaleo.com.

2.2 Duration

Processing will be done for the duration of the Master Contract.

3 Nature and purpose of collecting, processing or using the data

Apaleo stores and processes Personal Data to provide the Service and related technical support, as described in **Appendix 1**.

4 Obligations of Apaleo

- (1) Apaleo will only process Personal Data as contractually agreed or as instructed by you, unless we are legally obliged to carry out a specific type of data processing. In this case, we will inform you thereof prior to processing the data, unless informing you is illegal. We will not use Personal Data provided for processing for any another purpose, specifically our own.
- (2) We are aware of the applicable legal provisions on data protection, and will observe the principles of correct data processing.
- (3) We will maintain strict confidentiality when processing the Personal Data.
- (4) Any individuals who could have access to the data processed on behalf of the Customer are obliged in writing to maintain confidentiality, unless they are already legally required to do so via another written agreement.
- (5) Apaleo ensures that employees processing Personal Data have been made aware of the relevant data protection provisions as well as this DPA before starting to process the data. We regularly train and sensitize employees processing Personal Data, and ensure they are adequately instructed and supervised on an ongoing basis in terms of fulfilling data protection requirements.
- (6) In connection with the commissioned data processing, Apaleo will support the Customer when designing and updating the list of processing activities and implementing the data protection assessment. All data and documentation required will be provided and immediately made available to the Customer upon request.
- (7) If the Customer is subject to the inspection of supervisory authorities or any other bodies, or should affected persons exercise any rights against you, we will support you to the extent required, if the Personal Data being processed on behalf of the Customer is affected.
- (8) We will only provide information to third parties with your prior consent, and will immediately forward you inquiries sent directly to us.
- (9) Apaleo has appointed a data protection officer, who you can contact directly under privacy@Apaleo.com. Up to date contact information will be available on www.Apaleo.com.
- (10) Any data processing may only be carried out in the EU or EEC or, if the Subcontractor provides the agreed service outside the EU/EEA, the Supplier shall ensure compliance with EU Data Protection Regulations by appropriate measures.

5 Technical and organisational measures

- (1) **Appendix 2** describes the technical and organisational measures Apaleo takes to protect Customer Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access.
- (2) We may update our technical and organisational measures from time to time, but only in a way that will not result in the degradation of the overall security of the Service and Customer Data. We will inform you when that happens. Significant changes will only be done when the Parties agree.
- (3) Should the security measures implemented by Apaleo not, or no longer, be sufficient, we will inform you immediately.
- (4) Apaleo ensures that Personal Data processed on behalf of the Customer is kept strictly separate from any other data.

6 Stipulations on correcting, deleting and blocking data

- (1) Apaleo will only correct, delete or block data processed on behalf of the Customer, if this is in accordance to the Agreement, or when instructed by the Customer. If an individual person contacts us directly with such an instruction, we will forward the request to you.
- (2) Apaleo shall comply with the respective instructions provided by the Customer at all times and also after the termination of this DPA.

7 Subcontracting

- (1) Subcontractors may only be appointed on an individual basis with the Customer's written consent as explained in paragraph 6 of this article.
- (2) Consent is only possible if the Subcontractor is subject to a contractual minimum of data protection obligations, which are comparable with those stipulated in this DPA. The Customer can inspect the relevant contracts between Apaleo and the Subcontractor upon request.
- (3) The Customer's rights must also be able to be effectively exercised against the Subcontractor. The Customer must have the right to carry out inspections, or have them carried out by third parties to the extent specified here.
- (4) Subcontractors who are not located and do not operate exclusively within the EU or EEC, can only be appointed, if they meet data protection standards comparable to this DPA. We will provide you with information about the specific data protection guarantees provided by the Subcontractor and how evidence thereof can be obtained.
- (5) Apaleo will only transfer data processed on behalf of the Customer to the Subcontractor, after all conditions for appointing a Subcontractor have been met.
- (6) The Customer agrees to the appointment of the Subcontractors described in **Appendix 3**. A list of our current Subprocessors is available at or such other website as Apaleo may designate ("Subprocessor Page"). We may update the Subprocessor Page to reflect any changes in Subprocessors. We will provide thirty (30) days' prior written notice to you if you subscribe to receive notice via the mechanism on the Subprocessor Page. During this period you will have the opportunity to object on such change of subprocessor list.

8 Rights and obligations of the Customer

- (1) The Customer is solely responsible for assessing the admissibility of the processing requested and for the rights of affected parties.
- (2) The Customer shall document all orders, partial orders or instructions. In urgent cases, instructions may be given verbally. These instructions will be immediately confirmed and documented by Apaleo.
- (3) The Customer shall immediately notify Apaleo if it finds any errors or irregularities when reviewing the results of the processing.
- (4) The Customer is entitled to inspect compliance with the data protection provisions and contractual agreements with Apaleo to an appropriate extent, either personally or by third-parties. This includes obtaining information and accessing the stored data and the data processing programs as well as other on-site inspections. Apaleo must make it possible for all individuals entrusted with carrying out audits to access and inspect as required. Apaleo is required to provide

the necessary information, demonstrate the procedures and provide the necessary documentation for carrying out inspections.

- (5) Inspections at Apaleo's premises must be carried out without any avoidable disturbances to the operation of our business. Unless otherwise indicated for urgent reasons, which must be documented by the Customer, inspections shall be carried out after appropriate notice and during Apaleo's business hours, and not more frequently than every 12 months.

9 Notification obligations

- (1) Apaleo will immediately notify you of any Data Breaches, latest 24 hours from the moment we realise a Data Breach has occurred. This notification must contain at least the following information:
 - a. A description of the type of the Data Breach including, if possible, the categories and approximate number of affected persons as well as the respective categories and approximate number of the personal data sets;
 - b. The name and contact details of the data protection officer or another point of contact for further information;
 - c. A description of the probable consequences of the personal data protection infringement;
 - d. A description of the measures taken or proposed by Apaleo to rectify the personal data protection infringement and, where applicable, measures to mitigate their possible adverse effects.
- (2) Apaleo will immediately inform you of any inspections or measures carried out by supervisory authorities or other third parties if they relate to the commissioned data processing.
- (3) Apaleo will support you fulfilling your communication obligations towards affected persons of a Data Breach by providing all relevant information, in accordance with Art. 34 GDPR.
- (4) Apaleo supports the customer in complying with the obligations in Articles 32 to 36 of the GDPR for the security of personal data, reporting obligations in the event of data breaches, data protection impact assessments and prior consultations. These include obligation to:
 - a. ensure an appropriate level of protection through technical and organizational measures that take into account the circumstances and purposes of the processing as well as the forecast probability and severity of a possible violation of the law due to security gaps and enable an immediate detection of relevant violation events;
 - b. immediately report personal data breaches to the customer;
 - c. Support the Customer within the scope of his obligation to provide information to the data subject and to provide him with all relevant information immediately in this context;
 - d. assist the Customers in their data protection impact assessment;
 - e. support of the customer in the context of previous consultations with the supervisory authority.

10 Instructions

- (1) The Customer reserves the right of full authority to issue instructions concerning data processing on their behalf.
- (2) Apaleo will immediately inform the Customer if an instruction issued by the Customer violates, in its opinion, legal requirements. Apaleo is entitled to forego carrying out the relevant instructions until they have been confirmed or changed by the party responsible on behalf of the Customer.
- (3) Apaleo is to document the instructions issued and their implementation.

11 Ending the commissioned processing

- (1) When terminating the DPA or at any time upon your request, Apaleo will either destroy the data processed as part of the commission or submit the data to you at your discretion. All copies of the data still present will also be destroyed. The data will be destroyed in such a way that restoring or recreating the remaining information will no longer be possible, even with considerable effort.
- (2) Apaleo is obligated to immediately ensure the return or deletion of data from Subcontractors.
- (3) Apaleo must provide proof of the data being properly destroyed and immediately submit this proof to the Customer.
- (4) Apaleo will keep any documentation that serves the purpose of providing proof of proper data processing according to the respective retention periods, including the statutory period after the DPA has expired. We may submit the respective documentation to you once our contractual obligations have ended.

12 Jurisdiction, Law

- (1) The place of jurisdiction for any disputes arising from this Agreement shall be Munich, Germany.
- (2) This DPA and all appendixes related hereto shall be governed exclusively by the law of the Federal Republic of Germany.
- (3) By signing of this DPA Apaleo and the Customer agree that all previous DPAs cease to exist.

Munich,

.....

Customer

DocuSigned by: Philip von Dittfurth
DocuSigned by: Martin Reichenbach
EBA306AA01A2440... OFA3C498948247A...

Apaleo

Appendix 1 – Details of data processing

Apaleo stores and processes guest data on your behalf.

Data:

- ID/Passport data;
- Name;
- Email address;
- Address and communication data;
- Nationality;
- Gender;
- Date of birth;
- Free text comment (which technically can include personal data);
- Invoice address

Recipients: Apaleo employees working in product development and support can access this data, to provide support and help. This access is read-only, unless you request modifications or deletion of data in written form.

All Subcontractors are listed in Appendix 3.

Appendix 2 – Technical and organizational measures

See the sections *General Notes* and *Data processed on behalf (“Guest data”)* in the document Apaleo – Technical and Organizational measures.

Appendix 3 –Subcontractors

Subcontractors		
Tool	Purpose	Privacy Policy
Adyen N.V. (NL)	Apaleo uses Adyen's payment services to process payments on behalf of our customers from customers' guests. For this purpose, we give data regarding the means of payment (credit cards or information about other payment methods such as PayPal, Klarna or other providers) to Adyen N.V. Further, Apaleo ensures that the necessary data protection standards, such as PCI-DSS, are complied with and for this purpose Apaleo is subject to an annual external audit. Customer Success employees have access to the end users and customers personal data. The access is secured by a personal login.	https://www.adyen.com/policies-and-disclaimer/privacy-policy

Amazon Web Services EMEA SARL (DE)	app.Apaleo.com uses Amazon Web Services (AWS) as infrastructure. Thereby, personal data is stored and processed on AWS servers.	https://aws.amazon.com/privacy/
Contentful GmbH (DE)	Apaleo uses Contentful GmbH for the certification process for software solutions, storing data and information on the status of the relationships with the app solution.	https://www.contentful.com/legal/privacy-at-contentful/privacy-notice/
Datadog, Inc. (US)	Apaleo uses software from Datadog, Inc. to analyze the performance of app.Apaleo.com. For this purpose, personal data is processed to Datadog, Inc.	https://www.datadoghq.com/legal/privacy/ https://www.datadoghq.com/legal/datadog-eea-data-processing-addendum/
Functional Software Inc. (US)	Apaleo uses sentry.io for tracking and monitoring errors and problems when using app.Apaleo.com. For this purpose, personal data is processed to Functional Software Inc.	https://sentry.io/privacy/
Heroku Inc. (Salesforce) (US)	Apaleo uses Heroku Inc. (Salesforce) for the infrastructure, traces, creating of notes.	https://www.salesforce.com/company/privacy/ https://www.salesforce.com/content/dam/web/en_us/www/documents/legal/Agreements/data-processing-addendum.pdf
Hotjar Ltd.(MLT)	Apaleo uses Hotjar as an analytical tool for tracking the users behavior of the customers, trying to optimize the experience of the product. Hotjar is a technology service that helps us better understand our users' experience (e.g. how much time they spend on which pages, which links they choose to click, what users do and don't like, etc.) and this enables us to build and maintain our service with user feedback. Hotjar stores this information on our behalf in a pseudonymized user profile. Hotjar is contractually forbidden to sell any of the data collected on our behalf.	https://www.hotjar.com/legal/policies/privacy/ https://www.hotjar.com/legal/support/dpa/
Productboard Inc. (US)	Apaleo uses Productboard for improving the product and new features by obtaining certain customer insights, and managing roadmaps.	https://www.productboard.com/privacy-policy/
Usetiful - Dobbytec OÜ (EST)	Apaleo uses Usetiful as a layer over Apaleo product, and it helps the customer to navigate through the product.	https://www.usetiful.com/privacy-policy https://www.usetiful.com/gdpr
WP Engine, Inc. (GB)	Apaleo.com and store.Apaleo.com use WP Engine as infrastructure. Thereby, personal data is stored and processed to WP Engine.	https://wpengine.com/legal/privacy/ https://wpengine.com/legal/dpa/
Zendesk, Inc. (US)	Apaleo uses Zendesk Support and Zendesk Guide to provide users with support and documentation. Personal data is stored and processed to Zendesk. Inc.	https://www.zendesk.com/company/privacy-and-data-protection/#gdpr-sub

ZenHub - Axiom Labs Inc. (CAN)	Apaleo product development uses ZenHub as an internal tool, for providing pipelines, tracking issues.	https://www.zenhub.com/privacy-policy
--------------------------------	---	---

With all the subcontractors located in the U.S. Apaleo has signed data processing agreements which incorporate the Standard Contractual Clauses. This certifies their compliance with the EU GDPR.

Apaleo – technical and organizational measures

October 10, 2022

General notes

Awareness

Protecting the personal data we are entrusted with is very important to Apaleo. New functionality as well as changes in the overall architecture are discussed with by the security and privacy officer before they are implemented, to assess security risks and compliance. All members of the Apaleo product and support team received a software security and data privacy awareness training, which is refreshed at least once a year.

Data of customers and their employees, website visitors, leads and App providers

Controlled Access

Only Apaleo employees working in marketing and sales are allowed to access personal data of customers, website visitors, leads, and App providers. The master copy of all personal data is stored and processed using selected cloud software. Access is restricted via username and password, and when available multi-factor-authentication.

Only short-lived copies (typically hours, maximum 7 days) for fulfilling specific tasks that cannot be done using any of the selected cloud software can exist on electronic devices of members of the Apaleo sales and marketing team. Access to those devices is restricted minimum with user name and password, in some cases via biometrical identification.

Passwords need to adhere to a strict policy, which is regularly adopted to latest security standards.

Auditing

Modification of personal data is:

- logged by Hubspot (on a field level) and Microsoft OneDrive (on a document level)
- impossible in Microsoft Office 365. All user entered information is immutable.
- Not possible in zendesk, but data can be deleted. Employees have been briefed to not delete data without checking back with the privacy officer.
- Not audited and possible for all administrators in WP-Engine. The administrators have been briefed to not change the personal data provided by others.

Data processed on behalf (“Guest data”)

Controlled Access

Only Apaleo employees working in product development and support in Germany can access personal data. The master copy of all personal data is stored and processed using selected cloud software.

The protected system components are:

- 1) Elastic Container Services, object store (S3) and Relational Database Services in a secured production account of the Amazon Web Services (AWS)
- 2) Code Repository on Github.com
- 3) Build and Deployment Pipeline using Jenkins

Access to the protected system components is restricted via individual username and password, and when available multi-factor-authentication is enforced. The group of people with access to the certain system components is limited to a minimum and by proper configuration of access policies the access rights are also limited to those rights required to perform the job. The group of admins and the access policies are reviewed on a regular basis. Whenever an employee leaves the company all his accounts are deleted immediately.

The use of shared or default user ids is prevented, and default user ids are removed where possible. The passwords for the remaining default user ids are stored in a secure password vault only a limited group of people has access to.

Only short-lived copies (typically minutes, maximum 24 hours) for investigations of the support team can exist on electronic devices of members of the Apaleo support team. Access to those devices is restricted minimum with user name and password, in some cases via biometrical identification.

Passwords need to adhere to a strict policy, which is regularly adopted to latest security standards.

All data is secured on the transport layer (TLS) when transmitting data between different cloud applications or local computers. TLS protocols that are known to have security vulnerabilities will not be used.

Data at rest, that means, stored in the database, is encrypted.

Auditing

For the databases and object store, access and modifications are logged, including the user's identifier.

It is not possible to modify data through the used logging cloud services. Only the person designated to be on-call is supposed to access them, but access is not logged by these systems.

In Apaleo, access and modifications are logged, including a user identifier masked as 'support' for Apaleo product support members, as to not disclose employee data to customers. The support person on call can be identified via the on-call calendar. In exceptional cases, people who are not on-call will access this data, too. This will be documented in the calendar. If the customer request Apaleo support to modify or delete data processed on his behalf, this request will be documented in written form, including the person performing this task.

Data separation

Data of different customers is separated in the object store and databases. Test and productive data for a customer are separated. It is not possible to mix data for different customers within one request or response to the Apaleo APIs. Central components, mainly the Apaleo identity server, ensure that users of Apaleo can only access data for the customer projects they are members of.

Availability

Data in the database is additionally stored in close to real time on a fail-over replica. In case of an outage of the main database, this replica takes over within minutes.

Data stored in databases or object stores is backed up at least once a day, depending on the specific technology used. Backups are stored in a separate availability zone in the datacenters of Amazon Web Services, ensuring that problems in Apaleo's main zone of operations do not affect the backups. Backups of databases can typically be restored in less than one hour, backups of data in the object store within one day.

The outage of any of the components Apaleo consists of is constantly monitored, and problems will be reported to Apaleo after five minutes latest. For technical problems within the services, monitoring and reporting is done every 15 minutes.

Technical and organizational measures of Apaleo's subprocessors

We evaluate the security measures taken by each subprocessor, especially the ones processing guest data, before entering an agreement with them. With all the subprocessors located in the U.S. Apaleo has signed data processing agreements which incorporate the Standard Contractual Clauses as approved by the European Commission pursuant to its decision 2021/914 of 4 June 2021. This certifies their compliance with the EU GDPR. As the details are changing often, please refer to their documentation and compliance certifications, available online:

Subprocessor		
Tool	Purpose	Privacy Policy
Adyen N.V. (NL)	Apaleo uses Adyen's payment services to process payments on behalf of our customers from customers' guests. For this purpose, we give data regarding the means of payment (credit cards or information about other payment methods such as PayPal, Klarna or other providers) to Adyen N.V. Further. Apaleo ensures that the necessary data protection standards, such as PCI-DSS, are complied with and for this purpose Apaleo is subject to an annual external audit. Customer Success employees have access to the end users and customers personal data. The access is secured by a personal login.	https://www.adyen.com/policies-and-disclaimer/privacy-policy
Amazon Web Services EMEA SARL (DE)	app.Apaleo.com uses Amazon Web Services (AWS) as infrastructure. Thereby, personal data is stored and processed on AWS servers.	https://aws.amazon.com/privacy/
Contentful GmbH (DE)	Apaleo to use Contentful GmbH for the certification process for software solutions, storing data and information on the status of the relationships with the app solution.	https://www.contentful.com/legal/privacy-at-contentful/privacy-notice/
Datadog, Inc. (US)	Apaleo uses software from Datadog, Inc. to analyze the performance of app.Apaleo.com. For this purpose, personal data is processed to Datadog, Inc.	https://www.datadoghq.com/legal/privacy/ https://www.datadoghq.com/legal/datadog-eea-data-processing-addendum/
Functional Software Inc. (US)	Apaleo uses sentry.io for tracking and monitoring errors and problems when using app.Apaleo.com. For this purpose, personal data is processed to Functional Software Inc.	https://sentry.io/privacy/
Heroku Inc. (Salesforce) (US)	Apaleo uses Heroku Inc.(Salesforce) for the infrastructure, traces, creating of notes.	https://www.salesforce.com/company/privacy/ https://www.salesforce.com/content/dam/web/en_us/www/documents/legal/Agreements/data-processing-addendum.pdf

Hotjar Ltd.(MLT)	Apaleo uses Hotjar as an analytical tool for tracking the users behavior of the customers, trying to optimize the experience of the product. Hotjar is a technology service that helps us better understand our users' experience (e.g. how much time they spend on which pages, which links they choose to click, what users do and don't like, etc.) and this enables us to build and maintain our service with user feedback. Hotjar stores this information on our behalf in a pseudonymized user profile. Hotjar is contractually forbidden to sell any of the data collected on our behalf.	https://www.hotjar.com/legal/policies/privacy/ https://www.hotjar.com/legal/support/dpa/
Productboard Inc. (US)	Apaleo uses Productboard for improving the product and new features by obtaining certain customer insights, and managing roadmaps.	https://www.productboard.com/privacy-policy/
Usetiful - Dobbytec OÜ (EST)	Apaleo uses Usetiful as a layer over Apaleo product, and it helps the customer to navigate through the product.	https://www.usetiful.com/privacy-policy https://www.usetiful.com/gdpr
WP Engine, Inc. (GB)	Apaleo.com and store.Apaleo.com use WP Engine as infrastructure. Thereby, personal data is stored and processed to WP Engine.	https://wpengine.com/legal/privacy/ https://wpengine.com/legal/dpa/
Zendesk, Inc. (US)	Apaleo uses Zendesk Support and Zendesk Guide to provide users with support and documentation. Personal data is stored and processed to Zendesk. Inc.	https://www.zendesk.com/company/privacy-and-data-protection/#gdpr-sub
ZenHub - Axiom Labs Inc. (CAN)	Apaleo product development uses ZenHub as an internal tool, for providing pipelines, tracking issues.	https://www.zenhub.com/privacy-policy