TERMS AND CONDITIONS

OF PRESTASHOP HOSTING

Updates on September, 2024

PrestaShop is the designer and publisher of an open-source software solution, distributed under a free license (Open Software License OSL-3.0), allowing its users to create e-commerce sites.

This solution is available for download on the PrestaShop website www.prestashop.com.

It allows users to create and personalize their e-commerce site and add features, free or paid, freely developed by the PrestaShop community already integrated into the solution or accessible on the PrestaShop marketplace.

The benefit of the services of these T&Cs is exclusively reserved for professionals within the meaning of French consumer law. As such, it expressly acknowledges that it does not have the right of withdrawal enjoyed by consumers within the meaning of the Consumer Code.

These T&Cs govern the services provided by PrestaShop to its users. They form, with the PrestaShop personal data protection policy Hosting, the personal data subcontracting contract PrestaShop Hosting and the general conditions of use of “prestashop.com”, full terms of use.

PrestaShop reserves the right to modify these T&Cs at any time. If applicable, the modifications will take effect fifteen (15) days after their communication.

SUMMARY

1. Definitions

« **Addons** » designates the Modules and themes referenced and marketed within the Addons catalog.

« **Back Office** » designates the interface through which the Merchant or Technical service provider acting on behalf of a Merchant can administer and configure their Merchant Site and in particular add Addons.

« **Terms and Conditions of Use or T&Cs** » means these general conditions, including any annexes and modifications.

« **Host** » designates the accommodation provider Services.

« **Marketplace PrestaShop** » designates the platform referencing all Addons accessible at the address: https://addons.prestashop.com (or any URL which may be substituted for it).

« **Merchant** » designates any natural or legal person acting in a professional capacity and operating a Merchant Site.

« **Merchant Site** » designates the e-commerce site created by the Merchant using the Solution as well as lall data hosted with the Service.

« **Modules** » designates software developments carried out by PrestaShop or by a Seller intended to add one or more functionalities to the Merchant Sites, whether they are pre-installed or downloadable from la Marketplace PrestaShop.

« **Platform** » designates the space made available to the User allowing him to manage his Merchant Site(s) and in particular its hosting.

« **PrestaShop** » designates the limited company with capital of 580,852.35 euros, whose head office is located at 198 Avenue de France, in PARIS (75013), registered with the Paris RCS under number B 497 916 635.

« **Purchase order** » designates the commercial offer proposed by PrestaShop to the User to benefit from these Services.

« **Servers** » designates the Host's infrastructure made available to PrestaShop, connected to the Internet network and allocated to hosting the Merchant Site.

« **Services** » means the service(s) presented by these T&Cs.

« **SLA (Service Level Agreement)** » designates the level of service that PrestaShop undertakes to provide to Merchants and potential Users. It is detailed in Appendix 2.

« **Support** » means the technical assistance services described in the Appendix 2.

« Technical service provider » designates any natural or legal person acting in a professional capacity on behalf of a Merchant operating or wishing to operate a Merchant Site.

« Users » means any natural or legal person, Merchant, Technical service provider acting on behalf of a Merchant or seller using the Services subject to these T&Cs.

2. Purpose of the Service

The Service allows the User to benefit, throughout the subscription period, from access to the Platform and hosting of their Merchant Site(s) within the European Union with the Host.

The User therefore benefits from a license to use the Platform.

The User also benefits from Support, accessible 24h/24, 7j/7. This Support exclusively facilitates access and assistance in the operation of the Service by the User. However, it is not provided to compensate for the consequences of maneuvers or uses prohibited by these T&Cs or the Order Form.

The purpose of the Service is exclusively technical in nature.

3. Subscription to the Service

The Service is reserved for Users operating or managing a Merchant Site.

The User guarantees that all the information he communicates is accurate, sincere and up to date.

Each subscription to the Service is specific to the URL of the Merchant Site indicated on the Order Form.

The subscription is effective when the User has signed the Order Form and provided a payment method. PrestaShop then creates an account and provides the User with the username and password allowing them to access the Service.

4. Access and availability of the Service

The Service is made accessible by PrestaShop within a maximum period of thirty (30) days from the delivery by the User of the elements as detailed in Appendix 1.

PrestaShop will make its best efforts to make the Merchant Site accessible, 7 days a week, 24 hours a day and according to the commitments specified by the SLA in Appendix 2.

Access to the Server may nevertheless be closed by the Host in order to ensure the maintenance of the hardware and software necessary for hosting the Merchant Site.

PrestaShop informs the User by email at least 24 hours before any interruption of access to the Server.

In short,

The Service is accessible within thirty days from its subscription by the User. PrestaShop makes its best efforts to make the Merchant Site accessible 7 days a week, 24 hours a day.

Access may be suspended by the Host to ensure maintenance of the Service. The User will be notified 24 hours in advance.

5. Subscription duration

The duration of subscription to the Service is indicated in the Order Form and begins to run to count the delivery of the instance.

At the end of the initial subscription period, the subscription is tacitly renewed for the same period.

6. Financial conditions

6.1 Service payment

The price of the subscription to the Service is indicated in the Order Form.

It includes all taxes and is payable in euros.

Payment is made by monthly direct debit. The first monthly payment is deducted 30 days after the effective subscription date, the User will then be debited every month on the anniversary of the subscription date.

Each month started is due and cannot be refunded.

6.2 Price review

PrestaShop reserves the right to revise the price of the Service a maximum of twice a year and within the limit of 10% of the price excluding tax for each increase.

If applicable, PrestaShop informs the User of the revision at least 30 days before the new price comes into force. From this information, the User may request termination of the Service without penalty for 2 months; failing termination, the User is deemed to have accepted the new price.

In short,

Payment is made by monthly direct debit. The first monthly payment is deducted 30 days after the effective subscription date, the User will then be debited every month on the anniversary of the subscription date.

Each month started is due and cannot be refunded.

PrestaShop may revise the price of the Service up to twice a year and at most up to 10%

of the price. for each increase. The User is informed 30 days in advance of the change and may terminate the Service.

7. User Commitments

The User undertakes to :

- provide accurate data and up to date;
- ensure the confidentiality of its identifiers and access codes to the Platform. As such, he is therefore invited to modify, upon his first access to the Service, the password associated with his identifier by default.
- secure the hosted application and all the installations or configurations that it carries out on its Merchant Site (such as, in particular, the installation of Addons).

In the event of a security failure linked in particular to an application flaw or the misappropriation of access codes, the User must deploy without deadline all necessary means to correct the security breach and must inform PrestaShop concomitantly in order to remedy the security breach.

It is up to the User to manage the storage capacity to which he has subscribed in order to ensure the adequacy of this capacity to the volume of data to be stored. The User is also informed that if he decides to delete files, this deletion is definitive and the files cannot be returned.

Furthermore, the User undertakes to use the Service only for lawful purposes consistent with public order and good morals. It also undertakes to ensure that its technical service providers or employees respect the same obligations.

As such, the User is prohibited from:

- copy, rent, lease, sell, transfer, assign, sublicense, disassemble, reverse engineer or decompile (except to the limited extent expressly permitted by applicable law), modify or alter in any way either all or part of the Platform;
- take any action aimed at introducing a virus, worm, defect, Trojan horse, malware or other item of a destructive nature onto the Platform;
- use the Platform in a manner likely to cause nuisance, damage or loss to anyone, or harm, defame, abuse, harass or threaten others in any way or encourage any third party to engage in such conduct;
- use the Platform in any manner that may violate any law or regulation, or any third party right, including but not limited to intellectual property rights, privacy rights, and/or rights to confidentiality, or otherwise likely to harm PrestaShop.

The User will not attempt to access the private system areas of PrestaShop or other areas of the Platform to which he is expressly not authorized to access.

The User undertakes to take out professional liability insurance from reputably solvent insurance covering the risks linked to the use of the Service for the entire duration of use of the Services. The User undertakes to provide PrestaShop with said insurance upon simple request.

In short,

The User must provide accurate data and ensure confidentiality. It ensures the capacity of the adequacy of the volume of data stored in relation to the storage capacity to which it has subscribed.

The User undertakes to use the Service and the Platform in a lawful manner and in compliance with regulations, and as such, is prohibited from accessing unauthorized system areas.

The User undertakes to take out professional liability insurance. The latter can be requested by PrestaShop at any time.

8. PrestaShop Commitments

Throughout the subscription period, PrestaShop undertakes to provide the Service and to keep the User's data within the limit of the storage volume stipulated in the Order Form.

PrestaShop further undertakes to take all useful measures to guarantee the User that the data stored on the Servers is not accessible to third parties.

PrestaShop guarantees that the Host:

- implements all necessary security procedures to limit access to its installations and intrusions into the Server;
- regularly carries out compliance checks on the Server, checking physical and logical access and immediately correcting any anomaly encountered.

The characteristics of the Host's technical infrastructures may change provided that these modifications make it possible to offer performances at least equivalent to those provided at the time of signing hereof.

In the event that PrestaShop does not respect the performance levels of the SLA, the User may claim the penalties provided for in the latter and only in the form of a credit, to the exclusion of any damages, withholdings or cancellations of services. in progress. These penalties will not be due by PrestaShop in the event that this non-compliance results from mishandling, an error or a wrongful action attributable to the User, its employees, subcontractors or co-contractors.

It is understood that these commitments apply to Merchant Sites, PrestaShop making no commitment regarding the application or support for websites developed with a content management system (CMS) other than the Solution.

In short,

PrestaShop undertakes to provide the Service and store the data securely for the subscribed storage volume.

Prestashop guarantees that the Host has put in place the necessary technical measures to guarantee the security and compliance of the Servers.

Finally, in the event that PrestaShop does not respect the SLA levels for reasons attributable to it, the User can claim the penalties provided for in the latter (in the form of a credit).

9. Termination

9.1 Termination for convenience

At the end of the subscription period, the Service is tacitly renewed for the same duration.

The parties may terminate the Service by informing the other party by email or post to the address indicated in the Order Form sent two months before the end of the current subscription period.

In the event of termination after the deadline, the termination of the Service will occur at the end of the current subscription period. Consequently, the period following notification of termination of the Service will be considered to have expired and will not entitle the User to any reimbursement.

In short,

The Service is tacitly renewed for the same period as the subscription period. PrestaShop or the User may terminate by written notice sent two months before the renewal of the subscription to the other party. Termination ends at the end of the current period.

9.2 Termination for breach

The User acknowledges that PrestaShop may suspend the Service and/or terminate the User's subscription with immediate effect without prior notice and without notice, due to a serious breach by the User and in particular in the event of:

- non-compliance with the information mentioned on the Order Form,
- failure to comply after summons from the User, the form and/or content of the Site hosted on the Platform,
- non-payment of Service and invoices,
- more generally, any violation of these T&Cs.

The termination of the Service for breach does not entitle the User to any reimbursement for the period of subscription to the Service possibly remaining to be paid.

In short,

PrestaShop may suspend or terminate the Service with immediate effect in the event of non-compliance by the User with the information in the Order Form, a lack of conformity of the Merchant Site or any violation of these T&Cs. As such, termination does not entitle you to a refund of the remaining period.

9.3 End of Services

At the end of the Services, for whatever reason, the User is responsible for migrating the data from the Merchant Site hosted on the Platform to any other server of their choice. As such, the migration of the Merchant Site is carried out at the User's expense.

The User is informed that a backup of the Merchant Site database as well as all files present in the production environment (excluding cache and files outside the root directory of the production server) are available for thirty (30) calendar days following termination of the Service.

At the end of this period, PrestaShop destroys the servers, documents and databases hosted as part of the Services.

In short,

In the event of termination for any reason, the User is responsible for migrating the data from their Merchant Site. PrestaShop keeps a backup of the Merchant Site database for 30 days following termination, after this period all information, data and servers are destroyed.

10. User Responsibility

The User is solely responsible for the management, in particular commercial, logistical, marketing and financial, of his Merchant Site as well as all data stored on the Merchant Site and to which PrestaShop remains completely independent.

The migration of the Merchant Site and data on the Platform is carried out exclusively by the User. He may, however, request PrestaShop to migrate the Merchant Site, under the conditions described in Appendix 1.

Furthermore, in the event of notification received by PrestaShop from a third party on the basis of article 6-I-2 of law n°2004-575 of June 21, 2004 on confidence in the digital economy requesting PrestaShop withdrawal of content from the Merchant Site hosted on the Servers, the User undertakes to respond within a maximum period of 24 hours upon receipt of the notification by PrestaShop. In the absence of a written response from the User within this period, PrestaShop reserves the right to temporarily or definitively suspend the content in dispute without liability being incurred.

The User is solely responsible for:

- the use he makes of the Solution and undertakes to use the latter in compliance with public order and good morals as well as to respect the legislation applicable to it;
- content hosted and distributed on its Merchant Site;

PrestaShop cannot under any circumstances be held responsible for the legality of the content hosted and distributed by the User and is not required to verify compliance with the legislation of the content of the Merchant Site. Any violation of the law arising directly or indirectly from the operation of a Merchant Site is the sole responsibility of the User.

PrestaShop may interrupt access or terminate the Services if it notices a violation of the law or receives a requisition from the public authority, a legal request or a third party claim which, in PrestaShop's opinion, may be sufficiently serious and justified.

Furthermore, PrestaShop reserves the right (i) to carry out targeted and temporary monitoring operations relating to the use of the Service; (ii) to interrupt access and/or terminate the Service in the event of failure on the part of the User to comply with the obligations defined in this article and (iii) to interrupt access to the Service in the event of a technical fault, denial of service or fraud on the Merchant Site or the Platform.

The User will also be fully responsible for any damage suffered as a result by himself, PrestaShop or any other person.

In short,

The User is solely responsible for the migration of his Merchant Site and the management of the latter.

He is responsible for the compliance of his Merchant Site as well as the content hosted on it with the regulations. PrestaShop reserves the right to carry out monitoring operations relating to the use of the Services and to suspend or terminate the Services if it notices an infringement.

The user is responsible for any damage suffered by himself, PrestaShop or any third party in this regard.

11. Responsibility de PrestaShop

PrestaShop's liability is limited to the provision of the Service.

Both PrestaShop and the Host cannot be held liable if the Server made available by the latter was unavailable for reasons of force majeure, including in particular the long-term failure of the public electricity distribution network, the failure of the public telecommunications network, the loss of Internet connectivity due to the public and private operators on which the Host depends.

In any event, PrestaShop cannot be held responsible for:

- direct or indirect consequences due to the defect of goods, installations and equipment belonging to the User or for which the User has custody or responsibility, other than the Service provided by PrestaShop;
- in respect of the content of the Hosted Data. The User undertakes to raise and guarantee PrestaShop against any complaint of any nature whatsoever which may be addressed to it relating to the content of the Data;
- any alteration of Data due to the intervention of a third party in the User's network likely to interfere with the collection and transfer of Data;
- outside of PrestaShop's control, any intrusion by third parties into the User's system, nor the direct or indirect consequences of such intrusion, nor any fault, negligence, or any act of the User or third parties;
- possible harm suffered by the User resulting from fraudulent access to the Data by a third party in possession of the User's identifier and associated password.
- in the event of modification by the User of his IT environment.

In general and by express agreement, PrestaShop's liability is limited only to direct damage resulting from its proven negligence. Indirect damage such as, without this list being exhaustive: operating loss, commercial damage, loss of customers, loss of order, loss of margin, loss of profit, damage to brand image, consequences of third party recourse and others, are expressly excluded.

In short,

PrestaShop is responsible for providing the Service, excluding cases of force majeure.

PrestaShop cannot be held responsible for the consequences of defective installations, hosted data, intrusions by third parties into the User's networks or modification by the User of their IT environment.

In general, PrestaShop's liability is limited to direct damage resulting exclusively from a fault of PrestaShop.

12. Intellectual property rights

12.1 No transfer of intellectual property rights

Use of the Services does not result in any transfer of ownership between the parties. PrestaShop and the User have no rights to the brands and distinctive signs of the other party.

Consequently, the User undertakes not to infringe in any way whatsoever the intellectual property rights held by PrestaShop, in particular relating to texts, photos, videos, data, posters, logos, brands and other elements reproduced on the PrestaShop sites and for its services.

The use of the PrestaShop brand in a domain name by the User is strictly prohibited. The User therefore undertakes not to use the registered PrestaShop trademark within the domain name and URL of their Merchant Site.

12.2 Intellectual property rights of the Merchant Site

The User is the sole owner of the content of the Merchant Site.

When the Service expires, PrestaShop returns to the User all the elements belonging to them as well as any backup copies of the Merchant Site.

In short,

PrestaShop remains the owner of all the brands and logos it owns.

The User is not authorized to use them, in particular in communications, advertising or register them in a domain name. The User can use the name PrestaShop to make commercial references.

The User is the sole owner of the content of the Merchant Site.

13. Confidentiality

Subject to the Article “Personal Data”, PrestaShop and the User mutually undertake to keep confidential all information and work provided to the other party within the framework of the Services, and undertake not to disclose it to any third party, other than employees or agents who need to know it, and to use this information only for the purpose of carrying out their respective obligations under the Terms.

They also undertake to ensure that this obligation is respected by their staff, under-processor or any third party who may be involved in the execution of the Services.

The obligation of confidentiality remains in effect for the entire duration of the Services and for a period of 2 years after termination of the Service for any reason whatsoever.

14. Personal data

Information relating to the collection and processing of personal data is detailed in the Personal Data Protection Policy attached to these T&Cs.

In order to provide the Services, PrestaShop is required to process data in the name and on behalf of the User. For this purpose, the parties detail in the Personal Data Subcontracting Contract presented in Appendix 3 processing carried out within the framework of the Services.

15. No solicitation of staff

The User undertakes not to make a job offer or hire, directly or indirectly, a member of PrestaShop staff for the entire duration of the Services and for a period of one (1) year from the end of their supply.

In the event of non-compliance with this clause, the User undertakes to pay PrestaShop a lump sum compensation corresponding to two years of remuneration for each member of the poached staff.

16. Cession

The User acknowledges that the subscription to the Service is exclusively personal and cannot be the subject of any transfer free of charge or for a fee.

In order to ensure the proper execution of the obligations imposed on it by these T&Cs, PrestaShop reserves the right to assign, transfer or bring to a third party, all or part of these T&Cs or to substitute a third party for all or part of their execution.

17. Force majeure

PrestaShop may suspend the Services in the event of the occurrence of an event beyond its control, a case of force majeure as defined by the case law of the French courts, or due to the action of a third party.

18. Independence of the Parties

The parties remain independent of each other. No stipulation of these T&Cs has the object or purpose of creating any partnership, mandate, representation or subordination between PrestaShop and the User.

19. Applicable law and attribution of jurisdiction

These T&Cs are subject to French law.

Any dispute that may arise from the interpretation or execution of these T&Cs will be submitted, prior to any legal procedure, to the mediation of a mediator designated by the most diligent party. If mediation is not successful, the dispute will be subject to the exclusive jurisdiction of the Paris Commercial Court.

ANNEX 1 - MIGRATION SERVICES BY PRESTASHOP AS PART OF THE SERVICE

Migration of the Website to the Host's Server

The migration service includes:

- modification of database connection parameters,
- correction of site URLs in database,
- import of merchant site content into a versioning system,
- import corrected data into the Prestashop Hosting database,
- import of site content into the Prestashop Hosting environments agreed between the Parties,
- test the viability of the site,
- support in putting the Merchant Site into production,

The migration service does not include:

- specific developments that the User wishes to add,
- the creation of a graphic charter or a theme,
- installations of Additional Modules,
- resolving anomalies on Modules,
- support for anomalies,
- travel to the Merchant Site,
- Merchant Site audits except within the framework of subscribed options (performance audit and SEO audit),
- answers to functional questions on the use of the Solution.

This list is not exhaustive.

Prerequisites

To carry out the migration, the User must first provide PrestaShop with the following elements:

- Back-office access (mandatory : URL admin, login and password),
- database access
- access to sources
- access to site sources
- ssh Root access to the client's production server
- List of third-party tools to which the store must connect (for example ERP)

Migration arrangements

It is up to the User to make any prior modifications and backups that may be necessary before migration.

The User is informed that the migration may result in the unavailability of their Merchant Site for the duration of the migration.

The migration service is provided from Monday to Friday, from 9 a.m. to 5 p.m. (French time) and excluding public holidays.

PrestaShop undertakes to communicate to the User the report produced before the final migration of the Merchant Site. Validation of the report by the User with the PrestaShop teams is a prerequisite for the final migration.

The User acknowledges that upon validation of the report, the Merchant Site will be migrated as is and accepts it as is. Consequently, PrestaShop cannot be held responsible for any malfunctions or modifications that occur after the final migration.

ANNEX 2 - SERVICE LEVEL AGREEMENT (SLA)

1. Purpose of this annex

PrestaShop provides Users with resources including:

- all system files that are necessary to run the technology in the application, such as the system library and system tools as well as one or more hardware equipment (cloud servers) (hereinafter the “***Base layer***”)

- And a "***Layer Service***" especially designed and optimized to host and develop Merchant Sites created with the Solution (the "***Platform***”). The Service Layer contains all the files that are part of the technology used. For example, MySQL or Apache files.

This Platform allows Users to benefit from hosting of their Merchant Sites with a professional host, according to the level of service described in this SLA.

Excluded from the Services are layer management « Client Application » containing all code files, content added or generated by the client application and Addons installed by the Client.
For example: PhP Symfony files or NodeJS files.

It is the responsibility of the User or its software supplier to maintain and complete the code and files of the Client Application.

This appendix describes the service level agreement (“***SLA***”) agreed between PrestaShop and the User. It also includes the processes, roles and responsibilities of the entities involved in providing the Service.

2. Overview of included services

2.1 Availability of the Service and penalties for non-compliance

Availability : the availability of the Base Layer and the Platform is measured and monitored on a monthly basis. Availability is limited to paid services.

Average repair time (“TMDR”, or “Objective Recovery Time (OTR)”) is the average time between the determination of an incident and the resolution of an incident. This includes both individual incidents and the complete reconstruction of an environment.

The Recovery Point Objective (OPR) is defined by business continuity planning. This is the targeted maximum period of data loss due to an error.

Commitments on the availability of the Base Layer and the Platform:

Service level	
Availability	99,9%
Average repair time	2 hours *
Recovery Point Objective	24 hours

* Business days (Monday to Friday), weekends and public holidays included

In the event that Prestashop does not meet the defined SLA, the following reimbursement regime applies:
A = (L - P)

% under target	**Credit to be applied to the following monthly bill**
$A \leq 0.5\%$	5%
$0.5\% < A \leq 1\%$	10%
$1\% < A \leq 2.5\%$	15%
$2.5\% < A \leq 5\%$	25%
$5\% < A$	50%

A = Departure of service availability as stipulated above
L = Availability of the service as stipulated above
P = The actual availability percentage

It is specified that the credit granted never exceeds 50% of the price of the subscription to the Service.

2.2 Support

To benefit from Support, the User must have a Prestashop Account or PrestaShop Addons.

In order to offer optimal support, PrestaShop distinguishes between “critical” support and “non-critical” support. :

- **critical support** includes all issues that interfere with the proper functioning of the Platform and require immediate attention for its operation. This includes malfunction of cloud infrastructure, network and provisioning systems that lead to proven disruption of the Services. These services are monitored 24 hours a day, 7 days a week. In case an error is detected, corrective action will be taken immediately.

- **non-critical support** refers to all other questions including all questions related to the use of the services offered, software support (hosting-related layer), configuration changes (not necessary to resolve critical issues).

Any Support must be requested exclusively from the address: https://support.prestashop.com/ and can be requested 24 hours a day, 7 days a week, for all support requests.

The User opens tickets through the Support platform by selecting the “PS” category Hosting".

Depending on the criticality of the request, the methods for taking requests into account differ as follows:

Premium Support	
Critical Support	
Support hours	9h/18h *
Response time	< 1 hour*
# of tickets (platform error)	Unlimited
# of tickets (User error)	3 tickets per month per project (billed by time spent if more tickets or if time allocated exceeds 1 hour)
TMDR	2 hours* for any unavailability related to the Base Layer
Recovery point objective	24 hours
Non-critical support	
Support hours	10x5**
Response time	< 3 working days**
# of tickets (platform error)	Unlimited
# of tickets (User error)	3 tickets per month per project (with billing based on time spent if more tickets or if time allocated exceeds 1 hour)

* Every day from Monday to Friday
**Working days (Monday to Thursday) 9:00 a.m. to 6:00 p.m. CET and Friday 9:00 a.m. to 4:00 p.m. CET, excluding public holidays

Covered by Support
Installation and configuration issues
● Compatibility questions when installing dependencies at the service layer,

● Best practices for configuring supported application dependencies, ● General questions about platform-related hardware and service layers.
Troubleshooting
● Identification of problems that prevent a system application from functioning on the Hosting Platform, excluding problems related to the Solution application or any additional functionality to the Solution; ● Provide solutions to known issues, ● Answer general questions from Users and refer to the documentation, ● Fix issues for supported Service-tier software that exhibits irregular or incorrect behavior, such as a database server or Server failure.
Not supported by Support
● General debugging of User applications, ● Modification of the platform to support unsupported applications or application dependencies, ● Rewriting the application code for compatibility with the platform, ● Modification and/or correction of third-party or Open Source software for compatibility with the platform.

2.3 Incident, problem and change management

An incident is defined as an unplanned interruption or reduction in the quality of a Service (service interruption). The objective of the incident management process is to restore normal operation of the Service according to the schedule as defined in this SLA. “Normal service operation” is defined as service within the SLA.

A problem is defined as the cause of one or more incidents. The cause is usually unknown at the time a problem is logged and Prestashop is required to investigate further.

Change management

“Change management” is responsible for managing change processes involving changes such as:

- Platform functionality not yet available in the user interface,
- Network specific implementations,
- User-specific fixes and software,
- The Prestashop teams in charge of the platform will assess the relevance of the various changes reported before possible implementation.

Process

In the event of an incident, the User must create a ticket and provide:

- all relevant information on the commercial impact,
- all technical or functional elements allowing PrestaShop to reproduce the incident or carry out investigations,
- the importance of the reported incident to ensure the incident is correctly classified.

With this information, the support team intervenes for follow-up.

During the entire resolution process, the incident ticket is updated with status information. The User is informed of these updates via automatically generated email notifications.

Monitoring and interventions

An extensive monitoring system is in place to keep track of all critical aspects of the Hosting Platform. In the event of technical problems, the necessary technical personnel are automatically informed of the interventions, 24 hours a day, 7 days a week.

System monitoring

The following list is a summary of actively monitored and tracked system parameters: bandwidth, cpu context switches, cpu load, cpu frequency, disk io, dns resolution, system interrupts, disk io latencies, kernel version, system load, container status, memory usage, network connectivity, time synchronization, memory paging, process count, swap usage, number of network connections, threads, uptime, connection to the Client system, zombie processes.

Application monitoring

Specific elements are additionally monitored depending on the technology used.

For example: database performance, page requests, application memory consumption, cache-hit ratios.

The target response time for each monitoring event that requires manual intervention by a technician according to the SLA.

2.4 Back-ups

Back-ups are offered according to the following terms:

Backup	Detail
Interval	1x / day
Retention period	Daily: up to 7 days Weekly: up to 1 month
Retention number	11 backups (7 x 1 + 4 x 1)
Time frame	24/7

2.5 Software updates

Web server updates or patching include all tasks to ensure that all systems remain protected against security breaches.

The Platform is updated every 3 months, with minimal downtime. Critical fixes are applied within 24 hours.

Server and container updates

Containers containing applications or customer data are made up of 3 layers:

- **The base layer** contains all the system files that are necessary to run the technology in the application, such as the system library and system tools. The base layer of each container will be updated at least once every three months with the latest stable patches and all security fixes. In case of critical bug fixes or security patches, the base layer is updated within 24 hours.

- **The service layer** contains all the files that are part of the technology used. For example, MySQL or Apache files. The service layer of each container is updated at least once every three months with the latest stable patches and security fixes. In case of critical bug fixes or security patches, the base layer is updated within 24 hours.

- **The client application layer** contains all code files and content added or generated by the client or client application. The Client Application layer is excluded from updates. *For example: PhP Symfony files or NodeJS files.* It is the User's responsibility to maintain and complete the code and files of the Client Application.

Patching policy according to the service layer concerned

Patching process	Layer concerned
The User is responsible for maintaining the application code (e.g.: patches for the Symfony framework)	User Application (code, data)
Automatic patching every 3 months Critical security patches within 24 hours	Technological layer (Apache, MySQL, etc.)
Automatic patching every 3 months Critical security patches within 24 hours	Base layer (file system)

App updates

Application patching is the responsibility of the User. Prestashop does not carry out any updates or validation of the configuration of the User's application. This includes all application codes and frameworks that have been delivered or created by the User or its application provider.

2.6 Security

The Platform is designed to protect Users against threats through:

- implementing security controls at each layer, from the host (physical or virtual) to the application,
- isolation of customer applications and customer data,
- The ability to quickly perform security updates without user interaction or minimal service interruption.

Technically, this translates to:

- isolation of customer data;
- isolation from network traffic;
- process isolation;
- management of entry and evacuation traffic by separate nodes.

ANNEX 3 - SUBCONTRACTING CONTRACT FOR PERSONAL DATA FOR PRESTASHOP HOSTING SERVICES

PREAMBLE

This Data Processing Agreement (hereinafter referred to as "**DPA**") relating to the Processing of Personal Data forms, together with the General Conditions of Use and the attached Personal Data Protection Policy, all the conditions applicable to the relationship between the User and PrestaShop within the framework of the Services.

As part of the Services, the User may be required to communicate Personal Data to PrestaShop. Within the meaning of Article 4, points 7 and 8 of the GDPR, the User is the Controller and PrestaShop is the Processor.

1. Definitions

In the context of the DPA, the following terms, when used with a capital letter, shall have the following meaning :

"**Personal Data**" or “**Data**” means any information relating to an identified or identifiable natural person (hereinafter referred to as "**Data subject**").

A natural person who can be identified, directly or indirectly, in particular by reference to an identifier, such as a name, an identification number, location data, an online identifier, is deemed to be an “identifiable natural person”, or to one or more specific elements specific to its physical, physiological, genetic, psychological, economic, cultural or social identity.

Personal Data are those entrusted by the User to PrestaShop with a view to their Processing on his behalf within the framework of the Services; they are listed in section 4 below.

"**Controller**" has the meaning given to it in Article 4 -7 ° of the Regulations. For the purposes hereof, the Controller is the User.

“**Regulation**” means Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 (also the General Data Protection Regulation “**GDPR**”).

"**Processor**" means the natural or legal person, public authority, department or other body which processes Personal Data on behalf of the User ; under the DPA, PrestaShop is the Processor.

"**Processing**" means any operation or set of operations carried out or not using automated processes and applied to data or sets of Personal Data, such as the collection, recording, organization, Processing. structuring, conservation, adaptation or modification, extraction, consultation, use, communication by transmission, dissemination or any other form of making available, reconciliation or interconnection, limitation, l 'erasure or destruction.

"**Breach**" means a breach of security resulting, accidentally or unlawfully, in the destruction, loss, alteration, unauthorized disclosure of Personal Data transmitted, stored or otherwise processed or unauthorized access. to such Personal Data.

Capitalized terms used but not defined in this Agreement shall have the meaning given to them in the General Conditions of Use.

2. Purpose

The purpose of this DPA is to define the conditions under which PrestaShop undertakes to carry out, on behalf of the User, the Personal Data Processing operations defined below.

As part of their contractual relations, the parties undertake to comply with the regulations in force applicable to the Processing of Personal Data and, in particular, the Regulations (as well as Law No. 78-17 of January 6, 1978 as amended "Informatique et Libertés”).

3. Duration of the DPA

This DPA shall enter into force upon subscription to the Services by the User and shall terminate upon termination by either party.

4. Description of the processing

- **Service provided** : PrestaShop is authorized to process on behalf of the User the Personal Data necessary to provide them with the Services subject to the General Terms and Conditions.

- **Nature of the operations carried out** : The services provided and during which PrestaShop may process the User's Personal Data are described in the General Terms and Conditions and in its Appendices.

- **Purpose of Processing** : The Processing is necessary for PrestaShop to fulfill its contractual obligations and to effectively provide the subscribed Services.

- **Personal Data processed** : Identification data, technical data, connection data, transaction data.

- **Data subjects concerned** : User having subscribed to the Services as well as his own clients.

5. Obligation of PrestaShop

5.1 Processing of Personal Data

PrestaShop is committed to:

(i) process Personal Data only for the purpose (s) which are the subject of the subcontracting,

(ii) process Personal Data in accordance with the instructions documented by the User. If PrestaShop considers that an instruction constitutes a violation of the GDPR or of any other provision of Union law or of the law of the Member States relating to data protection, it shall immediately inform the person in charge of the treatment. In addition, if PrestaShop is required to transfer data to a country outside the European Union, it must inform the User of this legal obligation before Processing, unless the law concerned prohibits such information for important reasons. of public interest,

The User is informed that he can send written instructions if these are consistent with the Services subscribed to.

(iii) guarantee the confidentiality of Personal Data processed under the DPA. In the event that PrestaShop is legally required to communicate Personal Data to an authority, it will inform the User beforehand, unless the law prohibits such information for reasons of public interest,

(iv) ensure that the persons authorized to process Personal Data under this DPA:

- undertake to respect the confidentiality of Personal Data;
- receive the necessary training in the protection of Personal Data,
- process Personal Data only for the purposes of the aforementioned Processing.

(v) take into account, with regard to its tools, products, applications or services, the principles of data protection by design and of data protection by default.

5.2 Subcontracting

The User authorizes PrestaShop to use subsequent Subcontractors to carry out specific Processing activities.

As part of the Services, the User is informed that PrestaShop has already used the following Subcontractors :

- For the purpose of hosting your Sites, PrestaShop uses DeltaBlue, a limited liability company under Belgian law, with registered office at Kempische Steenweg 293, box 34, 3500 Hasselt, Belgium, registered with the Register of Legal Persons (RPM) of Antwerp, district of Hasselt under company number 0543.425.375.
- For the management of its clients and prospects, PrestaShop uses the software "HubSpot", published by the company HubSpot Inc. - 25 First Street, 1st Floor, Cambridge, MA 02141 - USA and Google Ireland Limited - Gordon House, Barrow Street, Dublin 4, Ireland.

A contract for the Processing of Personal Data between PrestaShop and our Subcontractors ensures a level of protection and security in accordance with the applicable legislation on the protection of Personal Data.

In case of subsequent subcontracting, PrestaShop shall inform the User of any changes regarding the addition or replacement of other Subcontractors at least one (1) month prior to the change in order to give the User the opportunity to object to such changes.

When PrestaShop will use another Subcontractor, PrestaShop undertakes to ensure that the same obligations are imposed on such subsequent Subcontractor as those set out in this Agreement, in relation to the protection of Personal Data and in order for such Subcontractor to meet the requirements of the Regulation.

5.3 Data subjects affected by the Processing

Right to information of Data subject. It is the User's responsibility to provide the information to his clients concerned by the Processing operations when collecting Personal Data.

Exercise of individual rights. As far as possible, PrestaShop will help the User to fulfill its obligation to respond to requests for the exercise of the rights of its clients : right of access, rectification, erasure and opposition, right to limitation of Processing, right to data portability, right not to be the subject of an individual automated decision (including profiling).

5.4 Notification of Personal Data Breaches

PrestaShop notifies the User of any violation of Personal Data within a maximum period of seventy-two (72) hours after becoming aware of it and by email. This notification is accompanied by any useful documentation to enable the User, if necessary, to notify the data Breach to the competent data protection authority.

PrestaShop will indicate, to the extent that the information is available, the following:

- Nature of the incident;
- Date and time of discovery of the incident;
- Personal Data impacted;
- Measures taken directly to limit any further damage;
- Date and time when the incident ended;
- Structural preventive measures for the future.

5.5 Help

PrestaShop undertakes to help the User, as far as possible, so that it meets its obligations with regard to the aforementioned Processing concerning the performance of a possible impact analysis, for the notification of data Breach and for the exercise of rights to its clients.

5.6 Data output

In case of termination of the Services, the User will be able to recover his Personal Data in accordance with the provisions of Article 8 of the General Terms of Use.

5.7 Documentation

PrestaShop declares that it keeps a written record of all categories of Processing activities carried out on behalf of the User.

PrestaShop provides the User with the necessary documentation to demonstrate compliance with all of its obligations and to allow audits to be carried out by the User.

6. Obligations of the User

The User agrees to:

- document in writing any instructions concerning the Processing of Personal Data by PrestaShop, if specific instructions need to be given,
- supervise the Processing, including performing audits and inspections at PrestaShop,
- notify any violation of Personal Data subject to a legal notification obligation to the competent supervisory authority.

For the performance of the Services covered by this DPA, the User makes the necessary information available in his Personal Data Protection Policy.

7. Security measure

PrestaShop undertakes to put in place technical and organizational measures intended to guarantee the security and confidentiality of Personal Data against any unauthorized access, alteration, use, modification and disclosure during the provision of the Services.

As such, PrestaShop employees in charge of the proper performance of the Services covered by this DPA are subject to an obligation of confidentiality.

Taking into account the state of knowledge, the costs of implementation and the nature, scope, context and purposes of the Processing, PrestaShop and the User undertake to implement the appropriate technical and organizational measures in order to guarantee a level of security adapted to the risk.

The technical and organizational measures are described in the appendix 3 bis.

8. Responsibilities

The parties recognize the sharing of their responsibilities towards the User's clients, in accordance with article 82 of the GDPR.

The User acknowledges that PrestaShop is only liable for the damage caused by the Processing if it has not complied with the specific obligations to Subcontractors in the aforementioned Regulations.

Appendix 3 bis - Technical and organizational measures

1. Organizational security measures

1.1. Security Management

a. Security policy and procedures: Processor must document a security policy with regard to the Processing of Personal Data.

b. Roles and responsibilities:

I. Roles and responsibilities related to the Processing of Personal Data are clearly defined and allocated in accordance with the security policy.
ii. During internal re-organizations or terminations and change of employment, revocation of rights and responsibilities with respective hand-over procedures is clearly defined.

c. Access Control Policy: Specific access control rights are allocated to each role involved in the Processing of Personal Data, following the need-to-know principle.

d. Resource/asset management: Processor has a register of the IT resources used for the Processing of Personal Data (hardware, software, and network). A specific person is assigned the task of maintaining and updating the register (e.g. IT officer).

e. Change management: Processor makes sure that all changes to the IT system are registered and monitored by a specific person (e.g. IT or security officer). Regular monitoring of this process takes place.

1.2. Incident response and business continuity

a. Incidents handling / Personal Data breaches:
i. An incident response plan with detailed procedures is defined to ensure effective and orderly response to incidents pertaining to Personal Data.

ii. Processor will report without undue delay to Controller any security incident that has resulted in a loss, misuse or unauthorized acquisition of any Personal Data.

b. Business continuity: Processor establishes the main procedures and controls to be followed in order to ensure the required level of continuity and availability of the IT system Processing Personal Data (in the event of an incident/Personal Data breach).

1.3. Human resources

a. Confidentiality of personnel: Processor ensures that all employees understand their responsibilities and obligations related to the Processing of Personal Data. Roles and responsibilities are clearly communicated during the pre-employment and/or induction process.

b. Training: Processor ensures that all employees are adequately informed about the security controls of the IT system that relate to their everyday work. Employees involved in the Processing of Personal Data are also properly informed about relevant data protection requirements and legal obligations through regular awareness campaigns.

2. Technical security measures

2.1. Access control and authentication

a. An access control system applicable to all users accessing the IT system is implemented. The system allows creating, approving, reviewing and deleting user accounts.

b. The use of common user accounts is avoided. In cases where this is necessary, it is ensured that all users of the common account have the same roles and responsibilities.

c. When granting access or assigning user roles, the “need-to-know principle” shall be observed in order to limit the number of users having access to Personal Data only to those who require it for achieving the Processor’s Processing purposes.

d. Where authentication mechanisms are based on passwords, Processor requires the password to be at least eight characters long and conform to very strong password control parameters including length, character complexity, and non-repeatability.

e. The authentication credentials (such as user ID and password) shall never be transmitted unprotected over the network.

2.2. Logging and monitoring

Log files are activated for each system/application used for the Processing of Personal Data. They include all types of access to data (view, modification, deletion).

2.3. Security of data at rest

a. Server/Database security
   i. Database and applications servers are configured to run using a separate account, with minimum OS privileges to function correctly.
   ii. Database and applications servers only process the Personal Data that are actually needed to process in order to achieve its Processing purposes.

b. Workstation security:
   i. Users are not able to deactivate or bypass security settings.
   ii. Anti-virus applications and detection signatures are configured on a regular basis.
   iii. Users don't have privileges to install or deactivate unauthorized software applications.
   iv. The system has session time-outs when the user has not been active for a certain time period.
   v. Critical security updates released by the operating system developer are installed regularly.

2.4. Network/Communication security

a. Whenever access is performed through the Internet, communication is encrypted through cryptographic protocols.

b. Traffic to and from the IT system is monitored and controlled through Firewalls and Intrusion Detection Systems.

2.5. Back-ups

a. Backup and data restore procedures are defined, documented and clearly linked to roles and responsibilities.

b. Backups are given an appropriate level of physical and environmental protection consistent with the standards applied on the originating data.

c. Execution of backups is monitored to ensure completeness.

2.6. Mobile/Portable devices

a. Mobile and portable device management procedures are defined and documented establishing clear rules for their proper use.

b. Mobile devices that are allowed to access the information system are pre-registered and pre-authorized.

2.7. Application lifecycle security

During the development lifecycle, best practice, state of the art and well acknowledged secure development practices or standards is followed.

2.8. Data deletion/disposal

a. Software-based overwriting will be performed on media prior to their disposal. In cases where this is not possible (CD’s, DVD’s, etc.) physical destruction will be performed.

b. Shredding of paper and portable media used to store Personal Data is carried out.

2.9. Physical security

The physical perimeter of the IT system infrastructure is not accessible by non-authorized personnel. Appropriate technical measures (e.g. Intrusion detection system, chipcard operated turnstile, single-person security entry system, locking system) or organizational measures (e.g., security guard) shall be set in place to protect security areas and their access points against entry by unauthorized persons.

Annex 3 bis - Technical and organizational measures

1. Organizational security measures

1.1. Security management

a. Security policy and procedures: The Processor must document a security policy with respect to the Processing of Personal Data.

b. Roles and responsibilities:

i. The roles and responsibilities related to the Processing of Personal Data are clearly defined and assigned in accordance with the security policy.
ii. During internal reorganizations, layoffs and job changes, the revocation of rights and responsibilities and the corresponding transfer procedures are clearly defined.

c. Access control policy: Specific access control rights are assigned to each role involved in the Processing of Personal Data, on a need-to-know basis.

d. Resource/asset management: The Data Controller has a register of IT resources used for the Processing of Personal Data (hardware, software and network). A specific person is responsible for maintaining and updating the register (for example, the IT manager).

e. Change management: The Data Controller ensures that all changes to the IT system are recorded and controlled by a specific person (for example, an IT or security manager). This process is subject to regular monitoring.

1.2. Incident response and business continuity

a. Handling incidents / Personal Data Violations:
i. An incident response plan with detailed procedures is defined to ensure an efficient and orderly response to incidents involving Personal Data.
ii. The Processor will report to the controller without undue delay any security incident resulting in loss, misuse or unauthorized acquisition of Personal Data.

b. Business continuity: The Data Controller establishes the main procedures and controls to be followed to ensure the required level of continuity and availability of the IT system processing the Personal Data (in the event of an incident/breach of Personal Data).

1.3. Human resources

a. Staff Confidentiality: The Data Controller ensures that all employees understand their responsibilities and obligations relating to the Processing of Personal Data. Roles and responsibilities are clearly communicated during the pre-employment and/or induction process.

b. Training: The Data Controller ensures that all employees are properly informed of the IT system security controls that relate to their daily work. Employees involved in the Processing of Personal Data are also properly informed of the relevant data protection requirements and legal obligations through regular awareness campaigns.

2. Technical security measures

2.1. Access control and authentication

a. An access control system applicable to all users accessing the computer system is put in place. This system allows you to create, approve, review and delete user accounts.

b. The use of common user accounts is avoided. In cases where this is necessary, we ensure that all users of the common account have the same roles and responsibilities.

c. When granting access or assigning user roles, the "need to know principle" must be respected in order to limit the number of users with access to Personal Data to those who need it to achieve the Processing objectives of the Data Controller.

d. Where authentication mechanisms are based on passwords, the Processor requires that the password be at least eight characters long and conform to very strong password control settings, including length, character complexity and non-repetitiveness.

e. Authentication information (such as user ID and password) should never be transmitted unprotected over the network.

2.2. Logging et surveillance

Log files are activated for each system/application used for the Processing of Personal Data. They include all types of data access (consultation, modification, deletion).

2.3. Data Security at Rest

a. Server/Database Security
i. Database and application servers are configured to operate using a separate account, with minimum operating system privileges to function properly.
ii. Database and application servers only process Personal Data that is actually necessary to process to achieve its processing purposes.

b. Workstation security

   i. Users are not able to disable or bypass security settings.

   ii. Antivirus applications and detection signatures are configured regularly.

   iii. Users are prohibited from installing or disabling unauthorized software applications.

   iv. The system has timeouts for sessions when the user has not been active for a certain period of time.

   v. Critical security updates released by the operating system developer are installed regularly.

2.4. Network and communications security

a. Whenever access is made via the Internet, the communication is encrypted using cryptographic protocols.

b. Traffic to and from the computer system is monitored and controlled by firewalls and intrusion detection systems.

2.5. Backups

a. Data backup and restoration procedures are defined, documented and clearly linked to roles and responsibilities.

b. Backups benefit from an appropriate level of physical and environmental protection, consistent with the standards applied to the original data.

c. The execution of backups is monitored to ensure that they are complete.

2.6. Mobile/portable devices

a. Procedures for managing mobile and portable devices are defined and documented, establishing clear rules for their correct use.

b. Mobile devices that are authorized to access the information system are pre-registered and pre-authorized.

2.7. Application lifecycle security

During the development cycle, best practices, state of the art and recognized secure development practices or standards are followed.

2.8. Data deletion/disposal

a. A software overwrite will be performed on the media before disposal. In cases where this is not possible (CD, DVD, etc.), physical destruction will be carried out.

b. Paper and portable media used to store Personal Data are shredded.

2.9. Physical security

The physical perimeter of the IT system infrastructure is not accessible by unauthorized personnel. Appropriate technical measures (e.g. intrusion detection system, smart card-operated turnstile, single-person security entry system, locking system) or organizational measures (e.g. security guard) are put in place to protect security areas and their access points against the entry of unauthorized persons.