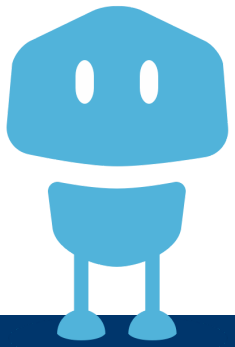
HYPERNODE®

by byte

Service Level Agreement



HYPERNODE®
by byte

Service Level Agreement 1

1. Introduction 3
- 1.1. Demarcation 3
- 1.2. Definitions 4

2. Role distribution between customer and Hypernode 6

3. Purchase of infrastructure from cloud providers 7

4. Available service levels 8

5. Uptime 9
- 5.1. Uptime guarantee on Grow plans 10
- 5.2. Uptime guarantee on Professional plans 10
- 5.3. Uptime guarantee on Excellence plans 11
- 5.4. Right to restitution 11

6. Backups 11

7. Security and Maintenance 12
- 7.1. Proactive monitoring 12
- 7.2. Software updates 13
- 7.3. Maintenance by Hypernode 13
- 7.4. Maintenance by suppliers 13
- 7.5. Urgent maintenance 13
- 7.6. Major maintenance 14
- 7.7. Security: technical measures 14
- 7.8. Security: procedural measures 14

8. Monitoring and support (including during disruptions) 15

9. Response time for business-critical disruptions 17

10. Recovery procedure for business-critical disruptions 17

11. Communication of disruptions 18

12. Hyperformance service and other temporary service provision 18

Digitrust MGMT. SYS. RvA C 618 ISO/IEC 27001

SELECT MAGENTO TECHNOLOGY PARTNER

1. Introduction

The supply of fast, secure and highly-available online stores is a collaboration between the customer, the hosting provider and any other suppliers involved. This Service Level Agreement (SLA) describes the service provision and guarantees that Hypernode's customers can expect of it as a hosting provider. The aim of this SLA is to be a quality guarantee from Hypernode to its customer(s). This SLA specifically covers hosting on the Hypernode platform developed by Hypernode.

Hypernode is ISO 27001-certified, which is an international standard for information security. The award of the ISO 27001:2013 quality label means that Hypernode's processes and procedures in respect of information security are very strict.

1.1. Demarcation

- Hypernode is responsible for the availability of the Hypernode platform and all Hypernodes running on the Hypernode.io domain.
- Hypernode is not responsible for service disruptions of third parties, which includes all its suppliers and the rest of the Internet.
- In certain cases, as summarised in section 5.0 of this SLA, service disruptions of suppliers where the Hypernodes are hosted will fall within the conditions for restitution.
- Hypernode and its suppliers shall in no event be held liable for consequential loss, including loss of earnings or savings, even if Hypernode had been informed of the possibility of such losses, nor are Hypernode or its suppliers liable for any claims by third parties.
- The Hypernode platform consists of all software developed on the platform by Hypernode and all cloud services provided and maintained by suppliers. The functioning of applications or sites that were not installed on the platform by Hypernode or by the cloud service provider fall outside the scope of this SLA.
- Hypernode shall not be liable for reduced performance as a result of malicious service disruption caused by third parties. This includes, but is not limited to, attacks by hackers.

- In cases of demonstrable negligence on the part of Hypernode, Hypernode shall be liable for an amount no greater than 40% of the monthly sum for the hosting contract to which the SLA pertains.
- The customer shall make responsible use of the services at its disposal and shall follow Hypernode's directions for responsible use quickly and effectively.
- This SLA is always entered into for the same contract period as the hosting contract to which it pertains and may be adapted to suit changing circumstances. The customer shall be notified of this by e-mail at least 1 month in advance, and is then entitled to terminate the agreement as of the next extension date.
- Hypernode's Terms and Conditions shall apply to this SLA. Hypernode's Terms and Conditions can be found on the website: www.hypernode.com. Where a stipulation in this SLA deviates from a stipulation in the Terms and Conditions, the stipulation in this SLA shall apply.
- Hypernode reserves the right to alter its pricing. The customer shall be notified of this by e-mail at least 1 month in advance.

1.2. Definitions

- Backup recovery: restoring one or more files to a new or existing Hypernode.
- Best effort: best effort means that Hypernode will strive to find the best solution as quickly as possible to the problems reported by the customer. But Hypernode offers no guarantees regarding the period within which these are realized. It is not possible to derive any rights from the proposed solutions.
- Business-critical disruptions: a disruption to the service provided by Hypernode, whereby the expected service is inadequate and the web shop is not available to customers.
- Contracting party: the person paying for the Hypernode plan and who therefore receives the quotation and the invoices. The contracting party is the entity with whom this SLA is entered into.
- Customer: someone who carries out the role of contracting party for the applicable Hypernode.

Digitrust MGMT. SYS. RvA C 618 ISO/IEC 27001
SELECT MAGENTO TECHNOLOGY PARTNER

- DDoS (attack): an attack from a large number of locations/computers (botnet) with the aim of making a computer network or service inaccessible to its users.
- Disruption/outage: a partial or total interruption of the expected service's availability, or a potential reduction to this.
- Downtime: see article 5: Uptime
- End-user: the owner of the online store for which the partner carries out technical management.
- First-line support: the tier of support that answers functional questions about the Hypernode company and its products and services. This includes plan recommendations, administrative queries, questions about settings in the Control Panel and questions on the functioning of our hosting and supplementary products/services.
- Hacker: someone who breaks into computer systems/websites or maliciously disrupts their effective functioning.
- Hypernode: a Virtual Private Server (VPS) on which a Magento application is hosted, including all software installed upon it by Hypernode.
- Hypernode emergency support service: The service that a customer can contact in the event of a disruption, available 24/7.
- Hypernode emergency support technician: The Hypernode technician who works outside of office hours to investigate, resolve and provide feedback on reported disruptions through the Hypernode emergency support service.
- Office hours: Monday through Friday, 9 am to 5:30 pm Dutch time, with the exception of public holidays.
- Partner: a Magento development agency that uses Hypernode's services to run multiple stores and has entered into a partnership with Hypernode.
- PKI: a technology for secure and trusted server communication over the Internet (or another public network) using digital certificates.
- Production hours: Monday through Sunday, 8 am to midnight Dutch time.
- Recovery time: The recovery time is the time between the detection of an incident confirmed by Hypernode and the moment when Hypernode has repaired the incident or proposed a workaround. Restoring a backup does not fall under recovery time as this depends on the amount of data to be restored.

Digitrust MGMT. SYS. RvA C 618 ISO/IEC 27001
SELECT MAGENTO TECHNOLOGY PARTNER

- Second-line support: the tier of support that answers technical questions about Hypernode's products and services.
- SSL: a technology for secure and trusted communication with websites on the Internet using digital certificates.
- Technician: a qualified member of Hypernode's technical staff, who can resolve disruptions independently.
- Technical manager: the person or organisation who carries out technical management of the store on behalf of the contracting party. This may also be the contracting party.
- Uptime: uptime is the time in which there is no downtime.

2. Role distribution between customer and Hypernode

Both Hypernode and the customer are responsible for the security and performance of the online store – each through their own expertise. The customer may be represented in this by a partner of Hypernode, in which case the customer themselves will be defined as an end-user. It could be said that Hypernode is responsible for everything at the server level, and the customer is responsible for everything at the application level. In practice, Hypernode will always make best efforts to examine and consider problems in order to resolve and/or prevent them if desired.

	Hypernode	Customer
First-line support for end-user by partner		✓
First-line support for partner	✓	
Second-line support for end-user and partner	✓	
Security at the server level	✓	
Security at the application level		✓

Digitrust MGMT. SYS. RvA C 618 ISO/IEC 27001
SELECT MAGENTO TECHNOLOGY PARTNER

Performance optimisation at the server level	✓	
Performance optimisation at the application level		✓
Availability monitoring and alerting if required	✓	
Taking action based on monitoring or alerting at the server level	✓	
Taking action based on monitoring or alerting at the application level		✓
Making tools available	✓	
Applying tools (such as e.g. caching)		✓

3. Purchase of infrastructure from cloud providers

Hypernode chooses external cloud providers and does this in the interests of stability, on a basis of good reputation and technical appraisal.

Hypernode monitors the performance and availability of the Virtual Private Servers it has purchased from these cloud providers 24/7. See the Monitoring and support section of this SLA for more information.

Hypernode only uses cloud providers that meet European personal data protection regulations. The cloud providers Hypernode works with meet all their legal obligations to store data securely and to offer customers operating around the globe the opportunity to move data internationally in accordance with European law.

Digitrust MGMT. SYS. RvA C 618 ISO/IEC 27001
SELECT MAGENTO TECHNOLOGY PARTNER

Hypernode uses a layered Access Control List for off-site backups. This allows us to separate access control to customer-specific data. In practice, this means: cloud servers have access solely to the specific customer's off-site storage.

The management of cloud servers takes place in line with the star/push model. Credentials are centralised. Changes are pushed to cloud servers, never pulled. A hypothetical security breach on a cloud server is thereby automatically isolated to a single instance.

4. Available service levels

Hypernode offers three different service levels. The Bronze SLA is included with all hosting plans on the Hypernode platform, with the exception of the Start hosting plan. From the Grow plan upwards, more extensive service levels can be chosen in the form of one of the SLA add-ons below.

	SLA Bronze	SLA Silver	SLA Gold
Monthly price, excl. VAT	Included as standard from the Grow plan upwards	€ 50	€ 100
Backup recovery: labour costs for making backup available **technical costs (see section 6 of this SLA)**	1 per month included calculated in arrears	1 per week included calculated in arrears	1 per day included calculated in arrears
Reporting disruptions	24/7	24/7	24/7
Response time for business-critical disruptions reported to Hypernode by customers	Best effort	<30 minutes	<30 minutes

Digitrust MGMT. SYS. RvA C 618 ISO/IEC 27001
SELECT MAGENTO TECHNOLOGY PARTNER

Telephone feedback from the emergency support technician outside of office hours	Not available	Not available	Included
Restore procedure for business-critical disruptions	Data recovery by client possible	Data recovery by client possible	Data recovery by client possible
Performance & security audit at customer request	Not included	Not included	1 per year
Communication of maintenance and disruptions	Via status.hypernode.com	Via status.hypernode.com	Via status.hypernode.com

Hypernode reserves the right to alter its pricing. The contracting party shall receive written notice of this by e-mail at least 1 month in advance.

5. Uptime

Downtime is classed as one of the following situations:

- The Hypernode is not accessible to external visitors owing to the unexpected or unintended failure of the software installed on the Hypernode.
- The Hypernode is not accessible to external visitors owing to a service failure with the supplier where the Hypernode is hosted. There are a number of exceptions to this.

The following situations would not be considered downtime:

- Force majeure, such as a power or network outage, DDoS attacks or other hacking activities.
- Planned maintenance works carried out by Hypernode, assuming this falls outside of production hours and does not extend to more than 8 hours per month.
- Planned maintenance works carried out by Hypernode's suppliers, assuming this does not extend to more than 8 hours per month.

Digitrust MGMT. SYS. RvA C 618 ISO/IEC 27001
SELECT MAGENTO TECHNOLOGY PARTNER

- Urgent maintenance required to maintain security and stability.
- Disruptions or outages caused by the customer, a colleague, or a third party acting on behalf of the customer.
- Application-related problems with applications or sites that were not installed on the platform by Hypernode, leading to disruptions/outages on the applicable website. The Magento sample store, which can be installed when booting the Hypernode if desired, also falls outside the scope of our responsibility.
- Hacked websites which, whether or not deliberately, have been disabled for this reason by Hypernode (or a third party).
- Affairs falling outside the SLA of the cloud provider where the Hypernode is hosted.

Downtime is recorded from the time at which (a) the customer reports a disruption or (b) Hypernode itself identifies it.

5.1. Uptime guarantee on Grow plans

Less than 99.5% uptime per month means that the SLA for Grow has not been met. Uptime is the total time in which there is no downtime. Uptime is calculated on a monthly basis. If the guaranteed uptime is not achieved, the contracting party may, at their own request, be refunded a percentage of the monthly cost for the hosting plan to which the SLA applies and where the uptime has not been achieved:

- Between 99.4% and 99.5%: 10% restitution of the monthly cost
- Between 99.3% and 99.4%: 20% restitution of the monthly cost
- Between 99.2% and 99.3%: 30% restitution of the monthly cost
- 99.2% or lower: 40% restitution of the monthly cost

5.2. Uptime guarantee on Professional plans

Less than 99.9% uptime per month means that the SLA for Professional has not been met. Uptime is the total time in which there is no downtime. Uptime is calculated on a monthly basis. If the

Digitrust RvA C 618 MGMT. SYS. ISO/IEC 27001
SELECT MAGENTO TECHNOLOGY PARTNER

guaranteed uptime is not achieved, the contracting party may, at their own request, be refunded a percentage of the monthly cost for the hosting plan to which the SLA applies and where the uptime has not been achieved:

- Between 99.8% and 99.9%: 10% restitution of the monthly cost
- Between 99.7% and 99.8%: 20% restitution of the monthly cost
- Between 99.6% and 99.7%: 30% restitution of the monthly cost
- 99.6% or lower: 40% restitution of the monthly cost

5.3. Uptime guarantee on Excellence plans

Less than 99.95% uptime per month means that the SLA for Excellence has not been met. Uptime is the total time in which there is no downtime. Uptime is calculated on a monthly basis. If the guaranteed uptime is not achieved, the contracting party may, at their own request, be refunded a percentage of the monthly cost for the hosting plan to which the SLA applies and where the uptime has not been achieved:

- Between 99.85% and 99.95%: 10% restitution of the monthly cost
- Between 99.75% and 99.85%: 20% restitution of the monthly cost
- Between 99.65% and 99.75%: 30% restitution of the monthly cost
- 99.65% or lower: 40% restitution of the monthly cost

5.4. Right to restitution

The contracting party becomes eligible for restitution in respect of downtime where they can demonstrate that Hypernode has not met the aforementioned performance obligations. In case of disagreement, the contracting party shall supply screenshots confirming that Hypernode's services are, or were, partially or wholly unavailable. The total restitution within a month may not exceed 40% of the monthly cost for the applicable plan to which the SLA applies.

Digitrust
MGMT. SYS. RvA C 618
ISO/IEC 27001
SELECT
MAGENTO TECHNOLOGY PARTNER

6. Backups

The following backup schedule applies to the Hypernode platform:

- 1 backup per day is available for the past 7 days: a maximum of 7 backups.
- Between 7 and 30 days, 1 backup per week is available: a maximum of 4 backups.
- Backups are available for up to 1 month prior.

We distinguish two types of cost for restoring a backup:

1. Technical costs: these are the costs of an extra Hypernode and the data transfer. These costs may vary according to the scale of the Hypernode required. These costs are always calculated in arrears and charged accordingly.
2. Labour costs for restoring a backup. Hypernode charges €100.00 per backup restore request.

- On the **SLA Bronze**, the labour costs for restoring a backup once per month are included.
- On the **SLA Silver** , the labour costs for restoring a backup once per week are included.
- On the **SLA Gold** , the labour costs for restoring a backup once per day are included.

7. Security and Maintenance

Hypernode undertakes to carry out preventative activities to reduce the chance of security incidents.

7.1. Proactive monitoring

Hypernode monitors the Hypernode platform 24/7/265. Scans shall be run to detect poorly-secured software and suspicious activities, among other factors. This strict monitoring allows for trends and patterns to be quickly discerned. This knowledge is then translated into new or improved processes to enhance the security and performance of the store, whereby issues can be prevented/resolved before coming to the customer's attention.

Digitrust MGMT. SYS. RvA C 618 ISO/IEC 27001
SELECT MAGENTO TECHNOLOGY PARTNER

With MageReport Premium, Hypernode exposes part of this monitoring to customers, such as long-running processes, CPU usage and Magento logs.

7.2. Software updates

When new versions of software installed by Hypernode are released, Hypernode carries out a risk analysis of (1) the risks to the platform; and (2) the impact on the functioning of the application. This informs the decision as to whether to (1) update immediately, without notification; (2) update immediately, with notification; (3) plan the update, with notification, or (4) if desired, provide a testing platform. Maintenance shall be announced by e-mail and/or at status.hypernode.com and, where possible, shall take place outside of production hours. Maintenance works shall not lead to reduced availability for more than 8 hours per month outside of production hours; any such hours shall not count towards downtime.

7.3. Maintenance by Hypernode

Maintenance shall take place outside of production hours, unless the estimated impact for customers is negligible or nil, in which case maintenance may take place within production hours. Maintenance shall be announced a minimum of 5 days in advance at status.hypernode.com.

7.4. Maintenance by suppliers

Supplier maintenance is maintenance that is planned and carried out by one of Hypernode's suppliers. Supplier maintenance may occur during production hours and may be announced fewer than 5 days in advance. Hypernode shall do everything in its power, on a best efforts basis, to encourage the supplier to announce maintenance in a timely manner and plan it around production hours. Supplier maintenance that impacts the uptime or performance of the Hypernode shall always be announced by Hypernode separately by e-mail and/or at status.hypernode.com, assuming the supplier has notified Hypernode of this in a timely manner.

7.5. Urgent maintenance

Hypernode may need to carry out urgent maintenance in respect of the stability of the entire platform, for example in cases of urgent security issues. Reduction in service or downtime as a result of such urgent maintenance shall not count towards downtime statistics. Urgent maintenance shall be carried out outside of production hours insofar as possible, but where necessary may also occur during production hours. Urgent maintenance shall always be explained at status.hypernode.com and by e-mail if necessary.

7.6. Major maintenance

Implementation of software with significant functionality changes shall be announced in advance by e-mail to the technical manager for the plan and at status.hypernode.com. Major version changes shall be announced a minimum of 30 days in advance.

7.7. Security: technical measures

All administrative actions shall be carried out over encrypted (SSL) connections.

- Mutual authentication between servers takes place by means of PKI.
- Customer passwords shall not be stored by us; only an encrypted representation of them. Should a hacker intrude into (parts of) Hypernode's systems, they would not be in a position to acquire our customers' passwords.

7.8. Security: procedural measures

- Hypernode follows the publication of security flaws closely. Based on internal guidelines, we shall estimate the chance of exploitation, impact of misuse and the functional impact on the solution. Where both the impact of misuse and the chance of exploitation are high, the flaw shall be patched immediately. Where this is not the case, and the implementation of a fix may have functional consequences for its customers' applications, the implementation shall

Digitrust MGMT. SYS. RvA C 618 ISO/IEC 27001
SELECT MAGENTO TECHNOLOGY PARTNER

be planned for the next maintenance window and an announcement shall be sent round to its customers.

- Hypernode's system passwords are changed at least every six months or upon the departure of technical staff.
- Any change to site, e-mail and customer data or domain ownership requires either password authentication or a written, signed confirmation of approval. Hypernode is particularly strict about this, considering it is the only way of preventing social engineering (manipulating Hypernode's staff into disclosing a password).
- Hypernode reactively scans log files for suspicious patterns. This enables Hypernode to detect misuse of any sites it hosts at an early stage.
- On a separate note, Hypernode also scans for suspicious software patterns. This allows Hypernode to warn its customers if they have installed insecure (older) applications that could potentially be misused to send out spam or to obscure a hacker's identity. This is an extra service from Hypernode to the customer. No rights or expectations can be derived from this.

8. Monitoring and support (including during disruptions)

The customer is entitled to telephone support during business hours. Hypernode shall respond to hosting-related support requests within 4 hours.

There is always, 24 hours per day, 7 days per week, 365 days a year a technician available for alerts from the monitoring system and for the emergency support service. Hypernode monitors the functionality of software installed by Hypernode across all Hypernodes, as well as the availability and stability of its cloud suppliers. Measurements are taken from various locations every minute. In the case of a disruption, these are forwarded directly to the 24/7 standby technician. This response time often means that Hypernode can resolve problems before customers notice them.

Digitrust MGMT. SYS. RvA C 618 ISO/IEC 27001
SELECT MAGENTO TECHNOLOGY PARTNER

All SLA plans allow for the customer to notify Hypernode of a disruption they have detected that is causing downtime 24/7.

- During office hours: by e-mail (support@hypernode.com) and/or telephone (+31 [0]20 521 6227).
- Outside of office hours: by telefoon (+31 [0]20 521 6627).

Once a disruption has been reported, the Hypernode emergency support technician shall take action to track down and resolve the issue. Whether direct contact (e-mail/telephone) about this is made between the emergency support service and the customer shall depend upon the SLA level. Because the emergency support service staff have access to each customer's individual technical record, which fully details the services they are using, Hypernode is able to offer rapid recovery times.

Where the Hypernode emergency support service is notified of a business-critical disruption outside of office hours, this shall be passed on to a Hypernode emergency support technician, who shall confirm receipt of the disruption notification with the customer. The guaranteed response time for this shall depend upon the SLA level purchased. The Hypernode emergency support technician shall then take action to track down and resolve the issue.

Having resolved the issue, the Hypernode emergency support technician shall confirm it as closed with the customer. From an SLA Gold level upwards, the Hypernode emergency support technician shall contact the customer directly by telephone to do so.

The Hypernode emergency support service's priority is to offer rapid support to prevent downtime for the customer's Magento application. Once the work has been completed, the Hypernode emergency support technician shall provide the customer with a debrief that can be used by the partner / web developer to resolve any remaining structural issues. Hypernode has a duty of obligation to resolve the submitted Magento application issue as well as possible ("best effort"). However, Hypernode can offer no guarantees of a solution. There are some problems we will not be able to resolve. In this sense, Hypernode's obligation is expressly not defined as result-oriented.

Where it becomes plain that the issue cannot be resolved quickly, the recovery procedure shall be commenced in consultation with the customer.

No rights may be derived from the solutions offered by Hypernode.

9. Response time for business-critical disruptions

The response time is the time between the detection of a disruption as confirmed by Hypernode (following an emergency support request) and the time at which Hypernode first communicates with the customer about the disruption. As part of this initial and subsequent communication, Hypernode shall keep the customer informed of any progress or results of the investigation carried out, and provide any available solutions or workarounds for the disruption. The response applies solely to this initial communication with the customer and not the resolution of the disruption itself.

10. Recovery procedure for business-critical disruptions

When Hypernode's monitoring produces an alert, the first thing to happen immediately is the commencement of the automatic emergency rescue procedure: alerts are followed by the necessary automatic emergency rescue strategy, which contains various actions such as restarting services, terminating processes, a reboot, etc. This is all with a view to resolving the issue.

When the issue cannot be resolved or when the customer reports a disruption, this shall be automatically escalated to the Hypernode emergency support service and the emergency support technicians shall commence troubleshooting.

In the case of a catastrophic failure of the original Hypernode (e.g. hardware, or through an unrecoverable software error on our side), a recovery procedure shall commence:

1. The Hypernode recovery will begin. Within 30 min. from commencement of the recovery, a new Hypernode shall be ready for use. This will be initially devoid of configuration or customer data.
2. The most recent backup of configuration and customer data shall then be restored. The data restore time will depend upon the quantity of data.

In case of booting a new Hypernode with a backup (owing to catastrophic failure of the original Hypernode), the customer may carry out data recovery themselves for any missing data created since the most recent backup.

11. Communication of disruptions

Where a disruption impacts upon multiple Hypernodes/customers, this shall be reported on status.hypernode.com.

- During office hours, a notification shall appear within 1 hours.
- Outside of office hours, a notification shall appear within 4 hours.
- Plans and alternatives shall be reported at status.hypernode.com within 2 hours during office hours, and within 6 hours outside of office hours.

12. Hyperformance service and other temporary service provision

Hypernode offers a number of services for which Hypernode staff will need temporary access to a store. For example, to raise its performance to the next level (the Hyperformance service) or to migrate the store from a different hosting provider. Arrangements for this shall be made with the customer and/or the partner in advance. In such cases, Hypernode shall not be responsible for the management, maintenance or future disruptions to the online store. Customers or partners shall

Digitrust MGMT. SYS. RvA C 618 ISO/IEC 27001
SELECT MAGENTO TECHNOLOGY PARTNER

not hold Hypernode liable for any present or future loss of earnings, costs incurred – whether or not by third parties – caused, for example (but not exclusively), by downtime or other disruptions as a result of a migration or other works carried out by Hypernode. Hypernode shall not be held liable for any defects, hacks or other problems that occur following Hypernode's temporary works. Naturally, we shall carry out these works with the utmost care, and shall be prepared to support the customer/partner where necessary.

Digitrust
MGMT. SYS. RvA C 618
ISO/IEC 27001
SELECT
MAGENTO TECHNOLOGY PARTNER