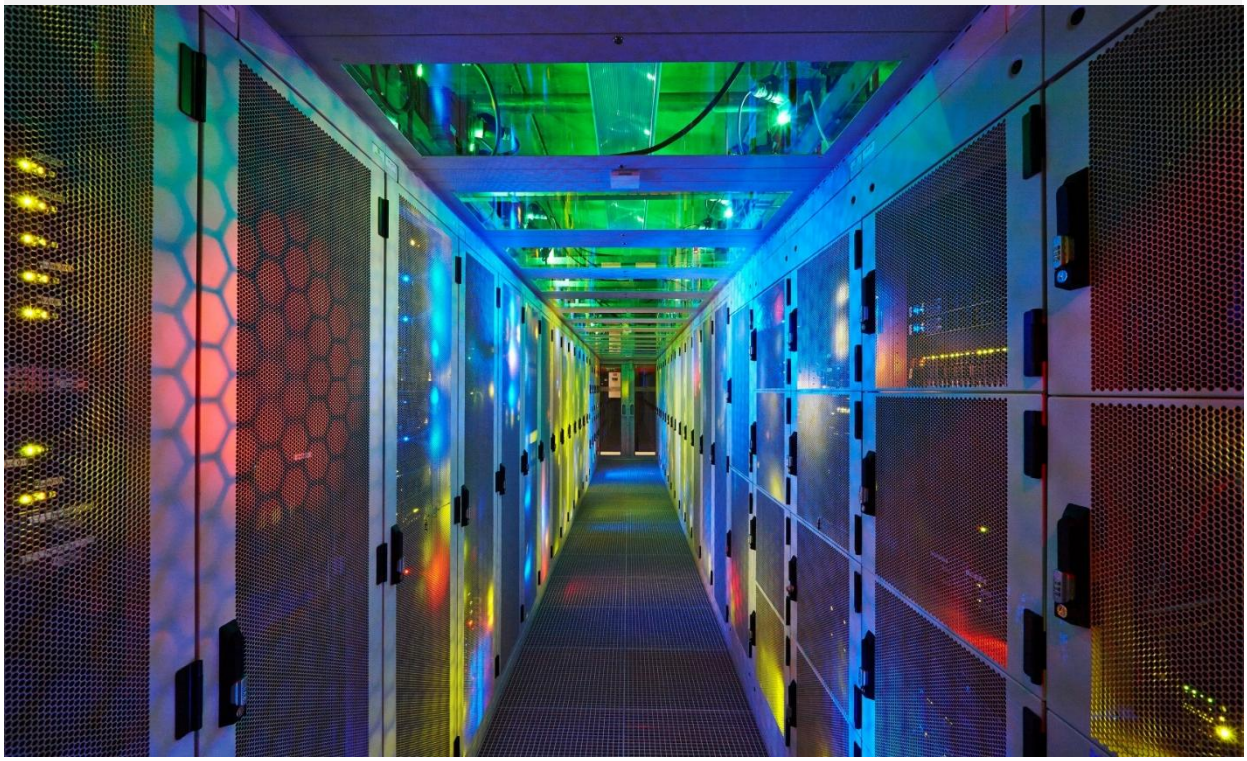
data place
datacenters

General Terms and Conditions & Privacy statement

Version 1.9

January 2021



GENERAL TERMS AND CONDITIONS

Article 1 Definitions

General Terms and Conditions:	These General Terms and Conditions.
Dataplace:	The party stated on the order form.
Customer:	The Party which has concluded an agreement with Dataplace under which it purchases one or more Services.
Agreement:	The agreement between Dataplace and the Customer consisting of an order form, the Service Description and the SLA and General Terms and Conditions.
Service:	The service described in the Agreement.
Dataplace Network:	The transmission equipment and, where applicable, the routing equipment and other technical equipment which enable the transmission of signals between connection points via cables, radio waves, optical equipment or other electromagnetic tools and insofar these are controlled by Dataplace.
Parties:	Dataplace and the Customer together.
Spam email:	Email which is sent in large quantities (bulk) and unsolicitedly. Unsolicitedly means that the receiver has granted no demonstrable and explicit permission for sending the email. Bulk means that the email is part of a larger amount of emails, which are essentially identical.
Confidential information:	All information pertaining to business affairs, prices, product developments, trade secrets, network information, know-how and (personnel) information of one of the Parties, as well as information which must reasonably be considered as confidential information of one of the Parties, and all information (in whatever form) which has been designated as confidential by the Parties.

Article 2 Explanation, Applicability and ranking

In the event of conflict between parts of the Agreement, the following ranking shall apply:

a. The order form (highest);
b. The service description and SLA;
c. The General Terms and Conditions (lowest).

Article 3 Conclusion of an agreement

1. The Agreement between Dataplace and the Customer will not be concluded until the signing of the order form by authorised representatives of both Parties.

Article 4 Delivery of the Service

1. After the Agreement is concluded, Dataplace will deliver the Service in accordance with the Agreement.

2. In order to enable delivery of the Service, the Customer will provide all the required documents, data, information carriers and other necessary materials to Dataplace completely, properly and in a timely manner. Dataplace must be notified in writing of any changes in data of the Customer (such as the invoicing address, office address and/or correspondence address and other administrative information) as soon as possible, and in any event no later than 2 weeks before the actual change takes place.

3. The Customer will observe all reasonable instructions from Dataplace concerning the delivery of the Service.

4. Dataplace does not warrant or represent that the Service it delivers is suitable for any other purpose than that set forth in the Agreement.

Article 5 Use of identification data

1. Dataplace will provide the Customer with identification data, address information and/or codes exclusively for the purpose of using the Service. The Customer will handle this identification data and address information and/or codes with care. Upon loss, theft and/or other forms of unauthorized use, the Customer will immediately inform Dataplace, so that the Parties can take appropriate measures.

2. If it may be reasonably assumed that third parties have misused identification data, address information and/or codes belonging to the Customer, Dataplace may give the Customer instructions, which must be complied with immediately. If the Customer does not immediately comply with these instructions, the Customer will be responsible toward Dataplace for any and all present and future loss/damage caused by the misuse.

3. If it has been established that the Customer has misused the identification data, address information and/or codes, the Customer will be responsible toward Dataplace for any and all present and future resulting loss and/or damage.

Article 6 Use of the Service

1. The Customer may not transfer the rights and obligations arising from the Agreement to any third party without prior consent in writing from Dataplace.

2. The Customer must ensure that it uses the Service and the associated terminal equipment with care. The Customer will comply with any reasonable instructions issued by Dataplace for the use of the Service and any associated terminal equipment.
3. The Customer may not use the equipment of software in such a way, or act in such a way, that may cause damage to the Service, to Dataplace or to third parties, or which may cause the Service to malfunction.

Article 7 Use of Dataplace Network

1. The Customer may use the Dataplace Network
2. The Customer will not cause any disruptions to the functioning of the Dataplace Network, network(s) of third parties and/or the connection between these networks.
3. The Customer indemnifies Dataplace against any and all claims, accusations or legal proceedings as a result of non-compliance with the provisions in paragraph 2 above, and will compensate Dataplace fully as and where applicable.
4. If Dataplace reasonably judges that the functioning and/or operation of the Dataplace Network and/or the services to Dataplace's customers is threatened, such as but not limited to spam email, open relay, port scan or hacking by the Customer and/or on the instructions of the Customer, Dataplace may give the Customer reasonable instructions, which must be complied with within the stated term.
5. The Customer is immediately in default, without notice of default being required, if the instructions referred to in the previous paragraph are not complied with and/or if (the contents of) the data traffic or the actions and/or omissions of the Customer are found to directly threaten the functioning of the Dataplace Network, networks of third parties or the link between these networks. The Customer is obligated to compensate all resulting loss and/or damage sustained by Dataplace.

Article 8 Customer's data traffic

1. If a third party notifies Dataplace that the Customer's website contains information which according to that third party violates the rights of that third party or which in any other way constitutes a wrongful act, Dataplace is entitled to immediately close the Service with which the website is connected to the Dataplace Network, or to immediately remove the information concerned from the system if the website is located on a Dataplace system, if it is probable that the disclosure of that information constitutes a wrongful act. Dataplace will never be liable for loss and/or damage of whatever nature caused by the Customer or its Customers as a result of service shutdown or removal of the information. Moreover, if justified by the severity of the violation, Dataplace will in that case be entitled to immediately terminate the Agreement, without any of the above giving rising to a right of compensation vested in the Customer against Dataplace.
2. The Customer indemnifies Dataplace against any and all claims, accusations or legal proceedings as a result of non-compliance with the provisions in paragraph 1 above, and will compensate Dataplace fully as and where applicable.

3. Dataplace maintains a 'fair use policy', meaning that the Customer may not use more bandwidth, whether or not occasionally, than is reasonably necessary for the Service and has been agreed with the Customer, the so-called 'bursting'. If the Customer exceeds this reasonably necessary bandwidth, which is stated in the Agreement, by more than 25%, Dataplace may charge the Customer separately for the resulting extra incurred costs.

4. Abuse reports about alleged spam activities from the IP addresses in use by the Customer will be forwarded to the Customer. The Customer is obligated to demonstrate within a period of 2 working days that the abuse report is not the result of spam activities. Failure to respond in a timely manner to abuse reports or responding without a plausible explanation may lead to termination of the Agreement.

Article 9 Privacy

1. Dataplace will comply with its obligations pursuant to privacy legislation Dataplace describes its processing operations as a data controller in its privacy statement. This statement forms part of this agreement. The statement may be amended from time to time. Dataplace will inform the Customer of any material change in the purposes of data processing. The Customer may give notice to terminate the agreement in writing within fourteen working days from the date of this notification, with effect from the date referred to in the notification by Dataplace on which the materially changed data processing is due to take effect..

2. Dataplace may provide information of the Customer to its affiliated enterprises, including parent company Eurofiber Group, which is necessary for delivering, or ensuring delivery, of the service.

3. Dataplace may include personal data of (employees of) customers in Dataplace's registration of persons, insofar as the data are strictly necessary for its administrative and management activities. This registration can only be accessed by Dataplace and is not provided to third parties, unless Dataplace is obligated to do so by law or court ruling.

Article 10 Confidentiality

1. The Parties agree to treat the Confidential Information which is exchanged in connection with the Agreement as strictly confidential. Neither Party will provide a third party with Confidential Information without express prior consent in writing from the other Party. An exception to this are enterprises affiliated to Dataplace, as set out in article 9.2 of this agreement.

2. All Confidential Information remains the property of the provider and will only be used by the receiving Party to execute the Agreement. All Confidential Information, including all copies thereof, must be returned to the provider or be destroyed as soon as the receiving Party no longer needs it, or as soon as the provider requests it be returned.

3. The provisions of paragraphs 1 and 2 above do not apply to Confidential Information which:
   a. becomes available in the public domain, other than by violation of this article by the receiving Party;
   b. has to be disclosed pursuant to a law, regulation, ruling or directive of a government or judicial body;
   c. has demonstrably been developed independently by the receiving Party; or
   d. becomes available to the receiving Party without any limitation or restriction imposed by a third party.

Article 11 Fee

1. The fees for the Service are due from the moment Dataplace notifies the Customer that the Service has been delivered.
2. In addition to this fee, Dataplace may charge the Customer for invoice specifications and itemisation, contract takeover, name changes and similar activities, insofar as these costs must reasonably be incurred.
3. Amounts as stated in the Agreement and in this article are in euros and are exclusive of VAT, unless stated otherwise.
4. In so far as the agreed fees are related to a certain period and are not payable for a full period, Dataplace will charge a proportional amount per calendar day.
5. Dataplace may amend the applicable prices and fees on the first day of a quarter, provided that Dataplace has notified the Customer in writing of the intended amendment not less than 30 days before the commencement of the respective quarter. If Dataplace wishes to reduce the applicable prices and fees, then Dataplace is entitled to do so immediately.
6. If the Customer does not wish to consent to an increase of prices and fees announced by Dataplace as referred to in paragraph 4 of this article, the Customer may give written notice to terminate the agreement within fourteen working days after the date of the notification referred to in these articles with effect from the intended effective date of the price or fee increase referred to in the notification by Dataplace.
7. Dataplace reserves the right to increase its prices per calendar year by a percentage equal to the increase of the Dutch consumer price index issued by the CBS in that year, with a minimum of three per cent. Notification of the aforementioned change by Dataplace will take place by no later than 31 March for the respective calendar year in which the indexation applies.

Article 12 Payment

1. Dataplace will invoice the Customer for the Service in accordance with the Agreement. Unless agreed otherwise, payment must occur within a term of 30 days from the invoice date. The moment of payment is the moment at which the payable amount has been received by Dataplace on its designated bank account. Any costs relating to the payment are for the Customer's account.
2. If the Customer believes that the invoiced amount is incorrect, the Customer must make its objections known to Dataplace in writing before the expiration date of the invoice. After receiving the objection, Dataplace will examine the correctness of the invoice amount. The part of the invoice amount which is not subject to objection remains payable. Payment of that part may not therefore be suspended.
3. All payment terms will always be strict deadlines. If the Customer fails to pay an amount payable by it in due time, it will be in default without any notice of default in that respect being required, and the Customer will be obligated to pay the statutory commercial interest from the invoice date.
4. If the Customer does not meet its obligations toward Dataplace, insofar as necessary after notice of default,

all judicial and extrajudicial costs related to the collection of the amounts owing will always be for the Customer's account. The extrajudicial costs amount to 15% of the principal amount payable, with a minimum of €250.

5. Payments shall first be applied toward payment of the interest due, judicial and extrajudicial costs, and thereafter toward payment of the oldest outstanding amounts receivable.

6. All amounts owing to Dataplace must always be paid by the Customer without the Customer being entitled to offset, suspension or deduction of whatever nature.

Article 13 Financial security

1. If, based on facts and circumstances, there may be reasonable doubt whether the Customer can meet its payment obligations and/or the provision of service(s) to the Customer will result in considerable investments for Dataplace, the latter is entitled to demand financial security from the Customer, such as the provision of a bank guarantee by the Customer, the pledging by the Customer of amounts receivable from third parties to Dataplace, or any other form of financial security.

2. The amount of the financial security referred to in paragraph 1 above will not be greater than the amount which the Customer will reasonably owe over a period of twelve months, in the opinion of Dataplace.

3. As soon as the need for provision of security is no longer present, based on the facts and circumstances, Dataplace will announce that the provision of financial security may lapse and be extinguished.

Article 14 Intellectual Property

1. All intellectual property rights vested in Dataplace or licensors will at all times remain the property of Dataplace or licensors.

Article 15 Force majeure and/or exceptional circumstances

1. Dataplace is not required to fulfil any obligation toward the Customer if it is prevented from doing so as a result of a circumstance which cannot be attributed to it or for which it is not responsible pursuant to the law, a legal act or generally accepted standards or practice.

2. Circumstances which are not attributable to Dataplace include, but are not confined to, transport delays, strikes, extreme weather conditions, riots, non-delivery or late delivery of services and/or products by their suppliers and/or malfunctions in a service and/or product of a supplier.

3. If the force majeure persists for longer than 60 days, the Parties may resolve in consultation to terminate the Agreement and make further arrangements regarding the resulting consequences.

Article 16 Liability

1. Dataplace's liability under an Agreement is limited to compensation of direct loss and/or damage and is limited to the total value of the Agreement, with a maximum in any event of EUR 10,000 per occurrence or

series of related occurrences and EUR 50,000 per year. Direct loss and/or damage exclusively means:

a. the reasonable costs the Customer has incurred in order to ensure Dataplace's performance conforms to the Agreement. However, these costs will not be reimbursed if the Customer has dissolved/terminated the Agreement;
b. the reasonable costs the Customer has incurred in order to assess the cause and extent of the loss and/or damage, insofar as the assessment related to direct loss and/or damage;
c. the reasonable costs the Customer has incurred in order to prevent or limit loss and/or damage, insofar as the Customer can demonstrate that these costs have resulted in limiting the direct loss and/or damage;
d. the reasonable loss and/or damage as a result of damage to goods or items belonging to the Customer, which was caused during activities carried out by or on behalf of Dataplace which are directly connected to the execution of the Agreement.

2. Dataplace;s liability for loss and/or damage resulting from death or personal injury is limited to the amount covered by the liability insurance taken out by Dataplace.

3. Dataplace is not liable for indirect loss and/or damage, including but not limited to loss and/or damage due to loss of usage time, reduced goodwill, data loss, lost profit, loss of savings, loss/damage due to interruption of business and any claims by the Customer's clients. It is the responsibility of the Customer to store its data in a sufficiently efficient manner, and to ensure back-ups are provided.

4. The limitation of liability referred to in this article does not apply insofar as loss and/or damage is a result of wilful misconduct or gross negligence committed by Dataplace's management personnel.

5. Apart from the cases referred to in this article, Dataplace cannot be held liable in any way for compensation, regardless of the grounds on which a claim for compensation and/or damages may be based.

6. A condition for the arising of any right to compensation for loss and/or damage is always that the Customer informs Dataplace of any loss and/or damage in writing as soon as possible after it arises. Compensation claims will expire by the mere lapse of 12 months after the claim arose.

Article 17 Suspension

Dataplace may suspend its obligations under the Agreement:

a. in the event of a shortcoming or fault (tekortkoming) on the part of the Customer, this being a structural violation of a material obligation under the Agreement, also including non-fulfilment of a payment obligation (in due time);
b. if the Customer has itself applied for a suspension of payments or has filed for bankruptcy, the bankruptcy has been declared or a suspension of payments has been granted to the Customer, a trustee or administrator has been appointed, or if the Customer is in any other way no longer capable of complying with the obligations toward its creditors.

Article 18 Term and termination

1. The Agreement may be terminated by means of a signed letter with effect from the end of the contract term, with due regard for the notice period in accordance with the Order Form, with the date on which Dataplace receives such letter being determinative in this regard.

2. A Party may only give notice of premature termination of the Agreement in writing by registered letter in the event:

    a. of any Shortcoming on the part of the other Party and such Party is in default in that respect;
    b. such Party is not able to comply with its (core) obligations under the Agreement as a result of Force Majeure for a period of sixty (60) days;
    c. the other Party has filed for bankruptcy or applied for a suspension of payments,
    d. the other Party is bankrupt or a suspension of payments has been granted;
    e. a trustee or administrator has been appointed for the other Party;
    f. of liquidation and/or winding-up of the legal person of the other Party;
    g. in the circumstances referred to in articles 9.1 and 11.5 of this agreement.

3. The termination of an Agreement will cause the rights and obligations of the Parties to terminate, on the understanding that the Customer is not entitled to repayment of the fee(s) which the Customer has paid Dataplace in advance.

4. In the event the Agreement is terminated, regardless of the reason:
    - Dataplace will, immediately following termination of the Agreement, withdraw the identification data, address information and/or codes it has provided;
    - Dataplace may charge the Customer (a) reasonable termination fee(s).

Article 19 Relocation

1. If prompted or justified by urgent circumstances, Dataplace has the right to relocate the Customer equipment. If reasonably possible, Dataplace will inform the Customer of this in advance.

2. The costs relating to a replacement or relocation as described in this article, including the costs for relocating Customer equipment, will be for Dataplace's account.

Article 20 Concluding provision

1. The articles which due to their nature are intended to remain effective even after the termination of the Agreement will remain in force after the termination of the Agreement.

2. If any provision, clause or condition in the Agreement is deemed void and/or non-enforceable by a court ruling, Dataplace is entitled to replace this provision by a similar provision which is legally enforceable, without this affecting the legality of the remaining provisions in the Agreement.

3. The Agreement replaces all prior commitments, arrangements and agreements between Parties regarding the Service in question.

4. Dataplace's records provide fully conclusive evidence between Parties, subject to proof to the contrary to be furnished by the Customer.

5. All disputes pertaining or relating to the Agreement are exclusively governed by Dutch law.

6. The District Court of Central Netherlands has exclusive competence to hear disputes and/or conflicts which may arise from or pertain to the Agreement, without prejudice to Dataplace's right to elect the Court in the Customer's place of domicile.

PRIVACY STATEMENT

Dataplace manages modern TIER III datacenters at multiple locations in the Netherlands. At these sites we co-locate large and not-so-large IT environments alike for a variety of different customers.

Inspired by a clear philosophy, centred on reliability, efficiency, sustainability and continuity, our datacenters operate to accomplish our mission: to provide continuity and high-quality datacenter services 24/7.

Some customers ask us for a **data processing agreement**. However, as we are not a processor of the personal data on your servers, we are unable to sign such an agreement. What we do is provide secure hosting for your servers. We explain this in the first section of this statement.

Under the General Data Protection Regulation, Dataplace is an independent controller for the processing of data about you, your employees and any suppliers, when you contact us, visit our website or when you or your employees require access to one of our datacenters. For further details, see the second section of this statement.

1. COLOCATION/HOUSING: DATAPLACE IS NOT A PROCESSOR

Dataplace offers organisations the possibility to co-locate their servers at one of our four datacenters in the Netherlands. Dataplace cannot access the personal data stored on your servers. Dataplace does not make any back-ups, nor does it provide any updates or maintenance for the operating system or applications running on your servers. The fact that Dataplace hosts your servers and provides you with a (fast) internet connection does not mean that Dataplace is a processor within the meaning of Article 4(8) of the GDPR. The co-location services that Dataplace provides are a form of transmission; Dataplace enables you to house your systems at a safe and secure location and ensures that your server can exchange data via the internet. However, Dataplace has no influence whatsoever on the processing of the personal data on, originating from or sent to your equipment.

Technical and organisational security measures

Dataplace takes appropriate technical and organisational measures to secure your servers holding personal data against loss or any form of unlawful processing. Dataplace ensures that these measures can be considered as providing an appropriate level of security within the meaning of the GDPR.

Various technical and organisational measures have been implemented both because it is in our DNA to do so and to meet our certification (e.g. ISO 27001 and NEN 7510) requirements. To retain our certification, Dataplace is obliged to review the measures at scheduled, regular intervals.

Employees' duty of secrecy

Dataplace is aware that our customers' servers may hold highly secret sensitive privacy and proprietary data. For this reason, all (permanent and temporary) employees of Dataplace must sign a separate non-disclosure agreement on commencing employment with us. Furthermore, each employment contract includes a non-disclosure clause. Dataplace additionally updates its employees at scheduled, regular intervals on the importance of complying fully with our privacy and security policy.

Strict access policy

Dataplace observes a very strict access policy. Dataplace uses physical as well as digital access control, records who entered and left the building at what times, and checks these logfiles at regular intervals. Digital control measures include general camera monitoring, digital registration for occasional visits or the issuing of badges for structural access rights. All visitors must register at the access terminal. An access badge may be issued to regular visitors, subject to certain conditions.

Responding to data incidents

Dataplace registers all security incidents and deals with them according to a standard procedure. Adherence to registration and our response to security incidents are assessed at regular intervals. In addition, incidents are analysed as part of our commitment to continuously improving our organisation. As well as this being part of our policy, we are also obliged to do so under the terms of our ISO 27001 and NEN 7510 certification.
Dataplace will provide you, as our customer, with timely, correct and full information on relevant data incidents, to enable you in your role as controller to meet your legal obligations to notify any data breach to the Dutch Data Protection Authority and also to inform the people affected (the data subjects), where applicable.

Dataplace will inform the contact person of the subscription/contract of a potential data breach. It is your responsibility as controller to keep the name and contact details of your contact person up-to-date via the Dataplace customer portal.

Examples of data incidents include irreparable damage caused to hard disks, theft of data on servers following a physical intrusion or successful hacking into the datacenter or a catastrophe, such as fire in a datacenter.

Dataplace will endeavour to provide you immediately, and in any event within 48 hours, with all the information which you need to make a complete notification, where necessary, to the Dutch Data Protection Authority and/or the data subject(s). If this information is not yet known, because the data breach is being investigated by Dataplace, for example, Dataplace will in any event provide you as soon as possible with the information which you need to make a provisional notification yourself to the Dutch Data Protection Authority and/or inform the data subject(s) within the stipulated 72 hours. Dataplace will inform you in any event about the nature of the (potential) breach, and where possible will provide a description of the observed and probable consequences of the breach and the action to be taken by you to mitigate and remedy the adverse effects of the data breach.

Dataplace will keep you (your contact person) informed about the progress and the measures that are taken. Dataplace will always inform you of any change in the situation and in the event further information becomes available.

In the event you, as our customer, make a (provisional) notification to the Dutch Data Protection Authority and/or the data subject(s) regarding a data breach at Dataplace, although it is quite clear to you that there is no data breach at Dataplace, you shall be liable for any and all loss and/or damage as well as costs sustained by Dataplace. You shall additionally be obliged immediately to withdraw such notification.

IaaS / Cloud services at Dataplace

With regard to IaaS / Cloud services, the applicable privacy laws and regulations require that additional agreements are made between Dataplace and the customer with regard to personal data. These agreements are laid down in a separate processing agreement that is concluded between Dataplace and its customers.

2. DATAPLACE AS INDEPENDENT CONTROLLER

Dataplace respects your privacy and ensures that all the personal data you give us, or which we collect about you, are treated as confidential.

You provide personal data yourself to Dataplace when you contact us by telephone or email, when you enter personal data about yourself via the customer contact portal and when you visit one of our datacenters. Dataplace also collects personal data about you when you visit our website, when your employer or client requests that you be enabled to access a datacenter and when you visit a datacenter. Dataplace only processes the personal data that are necessary to enter into and perform the agreement with you. Where it is required to do so by law, Dataplace will also provide personal data to competent authorities. And where Dataplace wishes to distribute newsletters to you or processes personal data via tracking cookies, we will first request your specific consent to do so.

Types of personal data

Dataplace keeps the volume of personal data of and about our customers that it collects to a minimum. Dataplace mainly collects contact and payment details. Dataplace does not collect any special categories of personal data of customers, as referred to in Article 9 and Article 10 of the GDPR, with the exception of your fingerprint (biometric data).
The data required to obtain (temporary) access to the Datacenter are:

- Your full name
- Your date of birth
- Your mobile phone number
- Your email address
- The number of your identity document
- A copy of your identity document
- The expiry date of your identity document
- Your fingerprint (not applicable in case of escorted access)

After authentication, the scan of your identity document will be deleted. Other information is stored in our systems in encrypted form. Dataplace uses your fingerprint as an additional means of authentication, to prevent unauthorised access. The fingerprint is saved on your access badge and stored in the access system in hashed form during your visit to the Datacenter. After leaving the Datacenter, your fingerprint is deleted from the system.. One month after your visit, your identity document number and its expiry date are erased. After 12 months, your name and date of birth also are erased from our systems.

If you have become a customer, you can enter data of your employees and suppliers via our customer portal to grant them access to the datacenter. The data required to obtain access to the Datacenter are the same as those listed above.

Dataplace has ensured that the systems cannot request or store the BSN (citizen service number).

Purposes

In summary, Dataplace processes the personal data referred to above for the following four purposes:

1. To enable authorised representatives of our customers to access their server equipment in one of our datacenters
2. To perform the services contractually agreed with you
3. To prepare and send invoices
4. To distribute by email service communications (not direct marketing)

Bases

The main basis for most processing of personal data is the need to conclude and perform the agreement. This also applies to the distribution by email of service communications. Dataplace will only provide personal data in response to a request by authorities such as the Netherlands Authority for the Financial Markets, the European Central bank or De Nederlandsche Bank N.V. where it is legally obliged to do so. They may require personal data for the performance of their tasks pursuant to the Dutch Financial Supervision Act (Wft). It is also possible that Dataplace is ordered to terminate the provision of its services by law enforcement or investigating authorities. In these cases, Dataplace processes personal data on the basis of mandatory compliance with a statutory obligation. Where Dataplace is jointly responsible with other organisations for the processing of personal data by allowing tracking cookies to be installed and read, Dataplace will first request your specific consent jointly on behalf of those other organisations.

Personnel and processors

As explained in the first section of this privacy statement, Dataplace considers it important that all its employees treat the personal data of its customers with due care. For this reason, Dataplace has all its (permanent and temporary) employees sign a separate non-disclosure agreement, for example.

Dataplace has also entered into data processing agreements with suppliers who process customers' personal data on our behalf, e.g. for the purpose of invoicing, access control, office IT systems and software development on the customer portal.

Transfer

Dataplace does not process any personal data of our customers outside the EU.

Security and responding to data breachs

Dataplace will, in case of doubt, always notify data breachs in its own systems and the systems of its processors and suppliers to the Dutch Data Protection Authority as well as the data subjects concerned._Dataplace relies on the GDPR and the guidelines of the European supervisory authorities concerning data breachs to determine whether a data breach has occurred. A data breach covers all security incidents causing the protection of personal data to

be breached or compromised at a given moment or resulting in the personal data being exposed to loss or unlawful processing.

Dataplace will notify potential data breachs within 72 hours to the Dutch Data Protection Authority. Dataplace will ensure that its employees are able to identify a data breach. Dataplace expects its processors and contractors to enable Dataplace to meet this commitment. For the sake of clarity: Dataplace will naturally also notify you, as our customer, of any data breach that occurs at a supplier of Dataplace. Dataplace is the point of contact for the customer. The customer therefore does not need to contact Dataplace's suppliers or processors.

Your rights based on the processing of personal data

The General Data Protection Regulation (GDPR) gives you certain rights to protect your interests where your personal data are processed, as follows:

- The right to data portability. The right to transmit personal data.
- The right to be forgotten.
- The right of access. This is the right of people to access the (your) personal data which are being processed.
- The right to rectification and supplement. The right to rectify the personal data you process.
- The right to restriction of processing: The right to temporarily stop the processing of the personal data.
- The right with respect to automated decision-making and profiling. Or: the right to human involvement in decision-making.
- The right to object to data processing.

How to contact us

If you would like more information, or if you have a complaint about how your personal data are used and/or treated, please contact Dataplace's quality manager. It is also possible to file a complaint with the Dutch Data Protection Authority (DPA). For further details: https://autoriteitpersoonsgegevens.nl/en

COOKIE STATEMENT

Dataplace uses cookies on its website to ensure the website functions properly and to help it understand how its website is used. To find out more, please read our cookie statement at www.dataplace.com/en/cookiebeleid

***