Registrar Agreement

Version 6.4

Applicable from 1 January 2027

Registrar Agreement

BETWEEN:

Organisation	Domain Name Registration Services België vzw, abbreviated DNS België vzw
Address	Engels Plein 35, 01.01 3000 Leuven Belgium
VAT number	BE 0466158640
Represented by	Philip Du Bois

Hereinafter referred to as "DNS Belgium",

AND:

Organisation	
Address	
VAT number	
Represented by	

Hereinafter referred to as "registrar",

WHEREAS:

DNS Belgium is the registration authority that manages domain names that end in .be;

The registrar wants to participate in the registration process of domain names ending in .be by registering or renewing domain names with DNS Belgium on behalf of its clients but for its own account;

DNS Belgium wants to co-operate with the registrar in registering and renewing the .be domain names under the conditions of this agreement;

THE PARTIES HAVE AGREED AS FOLLOWS:

Definitions

Registrar: a company, organisation or freelancer who provides domain name registration services for the .be name space to its customers.

Registrant: a natural person or legal entity applying for the registration or renewal of a domain name under the .be name space.

Terms & Conditions: the version of the terms and conditions for .be domain name registrations currently in force.

Bulk transfer: the transfer of (part of) a portfolio of .be domain names from one registrar to another.

Transfer lock: a lock placed on a domain name by the registrar to prevent that the domain name can be transferred from one registrar to another.

Domain Guard: a registry lock on a domain name that prevents any kind of change (update, transfer, deletion) to be made to the domain name. The activation and deactivation of this lock requires assistance from DNS Belgium.

Domain Shield: a registrar lock on a domain name that prevents any kind of change (update, transfer, deletion) to be made to the domain name. The activation and deactivation of this lock requires assistance from the registrar who manages the domain name.

Whois information: relevant information regarding the contact details of the registrant or other administrative or technical contact persons and which can be consulted via the search module on the DNS Belgium website.

Company number : for Belgian companies, this refers to the Crossroads Bank for Enterprises (CBE) number. For companies in other countries, it refers to the VAT number or an equivalent identification number.

1 Object

1.1 Right of use

According to this agreement, DNS Belgium will grant a right to use any domain name (insofar as it meets the registration criteria of the Terms & Conditions) under the .be domain (hereinafter referred to as the “domain name”), for which the registrar requests the registration or renewal is entered into its registration system by the registrar on behalf of its client but for its own account.

1.2 Non-exclusive right of use

The rights granted under this agreement are not exclusive. DNS Belgium will however not attribute any right for the registration or the renewal of domain names that were not introduced with DNS Belgium by a registrar, the provisions under article 9 excepted.

2 General Terms & Conditions

To obtain or renew a registration the registrar must:

- Ensure that the registrant has accepted the Terms & Conditions applicable when the application is made. The most recent version of these Terms & Condition can be found on: https://www.dnsbelgium.be/en/documents/enduser-terms-and-conditions-be
- Ensure that the registrant meets all requirements to obtain or renew a registration.
- Ensure that the contact details provided by the registrant are accurate and complete at the time of registration.
- Inform the registrant of all information the registrar receives from DNS Belgium that may influence the registrant and DNS Belgium's contractual relationship, particularly about an amendment of the terms & conditions.

3 Fees

3.1 Amount of fees

1. Once this agreement is signed, the registrar undertakes to communicate to DNS Belgium the prepayment amount (with an absolute minimum of € 2,500.00 (two thousand five hundred euros)) for the preparation of the initial advance invoice. The registrar is required to pay this advance invoice upon receipt and will only be allowed to enter paying transactions on DNS Belgium's technical systems once the payment of this initial advance invoice has been made.

2. The amount of the above invoice counts as a prepayment from which DNS Belgium will deduct the registrar's fees. The fees for new registrations are immediately deducted while the fees for the renewals are settled at the end of the month in which the registrations have been renewed. The other fees shall be deducted as soon as the task or transaction has been executed. When the balance of the prepayment reaches zero, the registrar may no longer carry out any new paying transactions (registrations, transfers, etc.). To prevent this, the registrar has to maintain its initial level of prepayment by paying the invoices for the registration and renewal fees issued by DNS Belgium in accordance with article 3.2.

3. The registrar must pay the registration, renewal and other fees for the domain names it registers, renews, transfers or manages on behalf of the registrants. Annex 1 sets out the various fees applicable under this agreement.

4. The registrar can request DNS Belgium to transfer all or a part of its domain names to another registrar. For these bulk transfers DNS Belgium will charge a specific transfer fee. The bulk transfer fee is set out in Annex 1.

5. The registrar shall be required to achieve the turnover figure in domain name transactions indicated in Annex 1. If the registrar fails to do so, DNS Belgium shall invoice the registrar for the difference between the target turnover and the turnover actually reached or terminate the agreement.

6. DNS Belgium may increase or decrease the fees and the turnover figure mentioned in the preceding paragraphs at any time and it will inform the registrar of any changes at least 30 days before the new fees become effective by e-mail and by publishing the new fees on DNS Belgium's website.

3.2 Terms and conditions of payment

1. The advance invoice mentioned in Article 3.1.1 must be settled upon signing this agreement.

2. The registration, renewal and other fees must be paid according to the terms and conditions of payment indicated in DNS Belgium's invoices to the registrar and shall in all cases be payable within 30 days.

   Invoices are issued at the end of each month for the registration, renewal and other transactions (transfer, reactivation, Domain Guard) relating to domain names carried out during the past month. The registrar must take all steps to delete every domain name not renewed by their registrant, from the automatic registration system at the latest on the last working day of that month. Domain names for which the right of use will expire during the month of invoicing and which are not deleted from the system will be automatically renewed and invoiced by DNS Belgium. The registration and renewal fees are due as soon as the right of use is granted or renewed, whether or not the registrant pays the registrar.

3. The bulk transfer fee must be paid according to payment modalities indicated by the specific invoice that DNS Belgium issues following the execution of the transfer of (part of) the portfolio.

4. Disputes regarding the invoices need to be notified in writing to DNS Belgium within 30 days of the invoice date. In case of late payment, the following penalties apply without notice: compensation payment of 10% of the amount due, with a minimum of 250,00 EUR, and a late-payment interest of 1% per started month, without prejudice to other sanctions in this agreement.

5. DNS Belgium shall use any received payments to settle the oldest outstanding and overdue invoices issued against the registrar.

4 Resellers

Under this agreement, the registrar may work with resellers. A reseller is any person or company which, whether on a contractual basis or not, has the possibility to register or renew .be domain names in the DNS Belgium registration system via an online interface or similar application provided by the registrar and which manages these domain names for several registrants. A reseller is not a person or company which only registers, renews or manages its own domain names via an online interface or similar application provided by the registrar.

However, the registrar is solely liable for observance of the provisions of this agreement. Possible infringements of the present agreement due to the behaviour of the resellers with which the registrar works, shall be considered as infringements of the registrar. Any registrar who works with resellers must therefore take the necessary actions to ensure the contractual obligations arising from the present agreement have legal effect vis-à-vis the resellers with which it works.

5 Technical provisions

5.1 Registration and other procedures

1. The registration procedure and most other procedures are fully automated through the technical platform of DNS Belgium. The registrar shall comply with the technical procedures developed by DNS Belgium for the registration or management of a domain name, as well as other technical and security requirements such as updating information about registrants while ensuring data confidentiality and integrity. DNS Belgium shall make a technical overview of the various procedures available to the registrars.

   The above provision applies in particular to:

   - the procedures, instructions and policies described in the manual for the .be registration system and of which it is not expressly specified that they are optional or recommended. The latest applicable version of the aforementioned manual is available on the DNS Belgium website: https://docs.dnsbelgium.be/;

   - any technical onboarding procedures and audits for registrars entering into an agreement with DNS Belgium for the first time from 1 January 2027. A description of the aforementioned procedures and audits is available on the DNS Belgium website: https://docs.dnsbelgium.be/

2. The registrar must have policies and procedures in place that allow to:

   - collect accurate and complete domain name registration data for the purpose of identifying and/or contacting domain name holders and administrative and technical contacts;
   - verify the above-mentioned data for accuracy and completeness;
   - periodically reverify the accuracy of the contact details of registrants and administrative and technical contacts and maintain records of these checks;
   - block the functionality of domain names if the above-mentioned data prove to be insufficiently accurate or complete;
   - give notice of default to the domain name holder or its administrative or technical contacts in order to correct and/or complete the above-mentioned data;
   - cancel domain names if the registrant or his administrative or technical contacts do not comply with the aforementioned notice.

   Insofar as DNS Belgium has already developed its own policies and procedures to fulfil the obligations contained in article 164/3 of the Act of 13 June 2005 on electronic communications, the registrar may refer to these policies and procedures instead of developing its own. DNS Belgium will publish the policies and procedures it has developed in this context on its website

3. If the registrar fails to comply with the procedures and technical and security requirements stipulated by DNS Belgium, the latter may decide to suspend the registrar temporarily by denying it access to the technical platform. If the registrar is suspended repeatedly, DNS Belgium may decide not to renew the agreement as provided under Article 8.

4. DNS Belgium shall be entitled to adjust or amend the registration procedure and other technical procedures at all times and shall inform the registrar no later than 30 (thirty) days before those adjustments or amendments become operational. At the same time, DNS Belgium must provide the registrar with all technical information required for their implementation.

5.2 Information security policy and reporting obligations

The registrar may not overload DNS Belgium's technical platform and network or hinder DNS Belgium from providing its services (for example by denial of service attacks). The registrar must not endanger the stability of the technical platform.

The registrar commits not to take any unlawful advantage of the "bugs and vulnerabilities" in DNS Belgium's technical systems that come to the registrar's notice neither to abuse them in any way. The registrar also agrees to report defaults such as mentioned above to DNS Belgium immediately. Under no circumstances will the registrar make these vulnerabilities public or disclose them to third parties. For our part, we at DNS Belgium guarantee a timely and adequate response to the reports that are submitted by the registrar.

The registrar applies all necessary and modern ('state of the art') cyber security and cyber hygiene techniques, at least (but not limited to) authentication and authorisation, encryption and system and network security, in order to minimise the risk and impact of incidents that could compromise the authenticity, integrity, availability or confidentiality of our services. The registrar also has a documented information security policy or is taking initiatives to develop one.

Notwithstanding the obligations set out in Article 6.1 of Annex 2, the registrar shall apprise DNS Belgium within 24 hours of serious incidents relating to cybersecurity that occur in his organisation. DNS Belgium shall treat this information with the utmost care and shall use it only to comply with legal (reporting) requirements.

If the registrar breaches these obligations, DNS Belgium may suspend this agreement immediately and without notice for 14 days. DNS Belgium may terminate the agreement if after 14 days the registrar still breaches these obligations.

6 Rules of conduct/obligations for the registrar

6.1 Registrant data

During the registration procedure, the registrar always states the details of the registrant or its representative and not its own details or the details of the reseller. The e-mail address shown in the contact information for the registrant is the address of the registrant itself or its representative and not the registrar's or the reseller's, except where expressly requested otherwise by the registrant.

Both during the registration procedure and afterwards, the registrar is solely responsible for the correctness of the details of the registrant. The registrar shall not register any details which it knows or suspects to be incorrect. The registrar shall immediately replace them by the correct details when it finds out or is notified by DNS Belgium or a third party that the details are incorrect.

The registrar undertakes to change the registrant's details, including their language preference, without delay at the registrant's or their representative's request. DNS Belgium reserves the right to

charge any costs it incurs to correct these details itself to the registrar who remains in default. The amount of these costs is indicated in Annex 1.

6.2 Prohibition on warehousing

The registrar is allowed to register domain names for its own use. Registrars must, however, refrain from 'warehousing' practices. Warehousing is the registering of large numbers of domain names for the registrar's own benefit. Registering large numbers of domain names on behalf of a registrant that is associated or linked with the registrar is also considered as 'warehousing' and hence is not permitted.

Under no circumstance may the registrar, directly or indirectly, introduce procedures, or take part in any such procedures, that are designed to sell domain names or to result in a change to the registrant of a particular domain name, except where the proper transaction is used that DNS Belgium provides for this type of operation.

6.3. Transfer lock and Bulk transfer

The registrar undertakes to solely lock a domain name using the transfer lock function at the registrant's request. The registrar may set this as a default function for all domain names it manages provided that the registrant is able to deactivate this locking mechanism easily and autonomously. DNS Belgium reserves the right to pass on any costs it incurs for the deactivation of the transfer lock function to the defaulting registrar. The amount of these costs is indicated in Annex 1.

The registrar must allow registrants to transfer their domain names to the registrar of their choice. The registrar must cooperate with the registrant, the new registrar and DNS Belgium for the transfer procedure.

When a request is made to set up a bulk transfer, the registrar may not unreasonably refuse its cooperation in this regard nor reject the request without justification.

6.4. Registrant verification

The registrar shall refrain from taking any actions to circumvent or prevent the implementation of the "Registrant Identity Verification" procedures established by DNS Belgium. The rules and functioning of these procedures are posted on www.dnsbelgium.be.

6.5. Unique registrar ID and prohibition on multiple IDs

The registrar may not create more than one registrar ID during the term of the agreement. The registrar ID constitutes the unique identifier used by DNS Belgium to identify the organisation as a registrar under the agreement.

The use of multiple or different VAT numbers does not entitle the registrar to create, register or maintain multiple registrar IDs. This restriction applies regardless of the number of VAT numbers held by the registrar.

If DNS Belgium determines that the registrar holds more than one registrar ID in violation of this provision, DNS Belgium shall be entitled to delete or deactivate the most recently created registrar ID without prior notice of default or notification. In such cases, DNS Belgium shall not be liable to pay the registrar any damages, compensation or other remuneration arising from the deletion or deactivation of the registrar ID concerned.

The provisions concerning the registrar IDs apply to new registrar agreements entered into with DNS Belgium from 1 January 2027. The aforementioned provisions do not apply in the context of any mergers and acquisitions involving .be registrars.

7 Protection of personal data

The registrar undertakes to comply at all times with all applicable data protection legislation with regard to all personal data that the registrar processes under this agreement.

If and to the extent that the registrar processes personal data under this agreement in a processor capacity on behalf of DNS Belgium, said processing shall be governed by the provisions stipulated in Annex 2.

8. Term

This agreement is established at the moment of its signature by the registrar. It will enter into force at the moment DNS Belgium receives the version signed by the registrar.

In principle the agreement is concluded for a period of one year. However, the first period will cover the period from the date of signing to 31 December of the year following the year in which the agreement was signed.

Afterwards the agreement is valid from 1 January to 31 December of every year. At the end of its term, the agreement shall be tacitly renewed every year for one year unless a party notifies the other party in writing no later than one and a half months before 31 December that it does not want to extend the agreement or wants to change the conditions of the agreement.

DNS Belgium shall at no time unreasonably refuse the tacit renewal but reserves the right to inform registrars of its intention not to continue the agreement if they fail to meet the minimum quality criteria, have insufficient technical knowledge to deal with DNS Belgium's technical systems, do not meet predefined security requirements (including cyber security and cyber hygiene), repeatedly fail to pay invoices on time, or elicit an unreasonably high number of complaints from registrants and third parties (relative to the number of registered domain names).

Without prejudice to the foregoing, DNS Belgium reserves the right to refuse registration and/or tacit renewal of the agreement where, in the light of the available information and the circumstances of the case, there are reasonable grounds to suspect fraud, abuse or an increased risk thereof.

DNS Belgium shall provide reasons for any such refusal, insofar as reasonably possible and without prejudice to its legal or contractual obligations.

9 Termination of the agreement

9.1 Termination of DNS Belgium’s registration authority

This agreement will terminate immediately if DNS Belgium is no longer authorized to manage the .be domain name zone for whatever reason. The registrar cannot hold DNS Belgium responsible for damage resulting from this termination, unless the termination is due to DNS Belgium's gross negligence or wilful misconduct.

DNS Belgium will immediately inform the registrar of any fact brought to its attention that may reasonably cause the termination of DNS Belgium's registration authority.

At the termination of its registration authority, DNS Belgium shall use its best efforts to:

- facilitate the continuation or the transfer of the existing contracts between DNS Belgium and the registrars at the termination date;
- obtain a notice period before the termination of its registration authority.

9.2 Breach of contract

If the registrar fails to fulfil its obligations under this agreement, DNS Belgium shall have the right to terminate the agreement if the registrar fails to comply with the written notice sent by DNS Belgium requiring it to fulfil its obligations within the period specified in that notice.

DNS Belgium shall also be entitled to suspend the performance of the agreement as soon as it becomes aware of a clear breach of the commitments undertaken by the registrar. In such a case, DNS Belgium will inform the registrar of the decision for temporary suspension and ask it to submit its arguments and any supporting documents within a period of 14 days so that they can be examined in detail by DNS Belgium with a view to revising or confirming the decision for temporary suspension.

As a result of the suspension, the registrar shall not be able to carry out any paying transactions (except for domain name renewals) on DNS Belgium's technical systems during this period.

If a breach is ascertained and is not adequately remedied by the registrar within the 14-day period, DNS Belgium shall be entitled to proceed to terminate the agreement as stipulated in the first paragraph of this article. In the case of minor infringements of the agreement or in situations where the registrar has a clear intention to remedy such infringements and/or avoid their recurrence, DNS Belgium shall refrain from terminating the agreement and decide to impose only a temporary suspension on the registrar.

9.3 Bankruptcy or judicial organisation

This agreement will terminate immediately if the registrar goes bankrupt or applies for a judicial organisation for his company (pursuant to the Companies Continuity Act of 31 January 2009).

9.4 Consequences of termination

Termination of this agreement shall result in the registrar losing access to the DNS Belgium registration system and no longer being able to enter domain name transactions. The registrar shall remain liable for payment of any fees due up to the date of termination.

DNS Belgium will transfer the domain names of the registrar whose agreement has been terminated to other registrars upon the request of that registrar or the person who is entitled to represent them. In such case DNS Belgium will charge the transfer fee that is mentioned in article 3.1.3 and will deduct the fee from the remainder of the prepayment that was paid in conformity with article 3.1.1 of this agreement. The possible remaining amount will be reimbursed to the registrar.

DNS Belgium may claim full compensation for the costs incurred, if they exceed the remainder of the prepayment.

10 Cooperation in audits and compliance management

10.1. General obligation

The registrar undertakes to provide all necessary cooperation in audits or similar 'compliance management' investigations of which DNS Belgium is the subject or which DNS Belgium itself organises as part of the verification of compliance with the contractual provisions relating to registrars. The registrar does not charge for the time spent on this cooperation. However, DNS Belgium will reimburse the costs resulting from special requests such as, for example, the delivery of specific certificates or the performance of specialised research.

10.2. Escalation measures in the event of non-compliance

If the registrar refuses to cooperate, fails to respond in a timely manner or provides incomplete information, DNS Belgium shall be entitled to take the following escalation measures, without prior notice of default and without being liable to pay any damages:

Administrative Suspension

If the registrar fails to comply fully with the compliance request within a reasonable period, DNS Belgium shall be entitled to suspend the registrar's access to the registration system.

Termination of the Agreement

If the breach has not been remedied within **90 days of the initial suspension**, DNS Belgium shall be entitled to terminate the agreement in accordance with the first paragraph of Article **9.2**.

10.3. Special provisions for cooperating registrars

If a registrar that cooperates in the context of the compliance procedure fails to comply with its contractual obligations but clearly demonstrates a firm intention to remedy the identified breaches and/or prevent their recurrence, DNS Belgium shall not seek to terminate the agreement. However, in such cases, DNS Belgium shall select the registrar for another compliance review the following year.

11 Assignment of rights

The registrar may assign rights under this agreement to a third party if the registrar informs DNS Belgium in writing no later than one month before the assignment becomes effective. The old registrar and the assignee are jointly and severally liable for performing this agreement until the end of the agreement with DNS Belgium.

If the registrar's company number changes, it shall have to create a new registrar ID and ask DNS Belgium to transfer all domain names and other elements linked with the current account to the new account. DNS Belgium shall not charge any costs for such transfer and will consider the feasibility of updating the existing account of the registrar rather than a migration to a new account (depending on compliance with tax regulations).

12 Guarantees

The registrar must indemnify DNS Belgium against any claim, in or out of court, from registrants or third parties regarding the products and services offered by the registrar or by DNS Belgium or regarding damages claimed from DNS Belgium, including claims for:

- Granting or not granting, renewing or not renewing the right of use to a registrant or a third party for a domain name, because for example, of an error regarding identity;
- Terminating DNS Belgium's registration authority of the .be domain name zone;
- Third parties claiming rights on a domain name;
- Technical defects or shortcomings.

13 Miscellaneous

13.1 Effect of this agreement on third parties

This agreement has only legal consequences for the signing parties and not for third parties. Therefor third parties cannot obtain any rights from this agreement, not with regard to the registrar, nor with regard to DNS Belgium.

13.2 Amendments

This agreement can only be amended with written consent of both parties. This does not apply to amendments to the registration, renewal and other fees which DNS Belgium may amend under this agreement.

13.3 Disputes

Only the courts of Leuven have the jurisdiction to handle disputes under this agreement.

The courts will apply Belgian law.

13.4 Intellectual property

This agreement does not change the status of any intellectual property rights of the parties. The parties will remain owners of their own intellectual property rights.

13.5. Human rights

The registrar (including any resellers with which it may work) endorses the principle that the protection and promotion of human rights and respect for fair working conditions are essential elements of responsible and sustainable business practices.

The registrar is encouraged to endorse the Code of Conduct drawn up by DNS Belgium for its suppliers and business partners. Alternatively, the registrar may also use its own code of conduct or policy document or one developed by a third party relating to human rights and working conditions, provided that the principles set out in DNS Belgium's Code of Conduct are incorporated and safeguarded to an equivalent standard.

13.6 Use of logos and name of DNS Belgium

The registrar has the right to use DNS Belgium's logo and name to the extent that it is intended to inform users of the contractual cooperation by and between the registrar and DNS Belgium. The registrar is expressly prohibited from using the logo and the name of DNS Belgium in a way that impersonates DNS Belgium itself or tries to create such an impression and thereby causes confusion for users and other interested parties.

If the registrar fails to comply with the foregoing provisions, DNS Belgium shall be entitled to require the registrar to cease the identified breach without delay and immediately upon first request and, where applicable, to remedy its consequences. Without prejudice to DNS Belgium's other rights and remedies, DNS Belgium shall also be entitled to claim compensation for any damage it has suffered as a result of the breach.

13.7 Contact details and website of the registrar

The registrar must ensure that the contact details notified to DNS Belgium are and remain correct. The registrar is obliged to inform any changes to these contact details without delay to DNS Belgium. Contact details shall explicitly be understood to mean: name, address details, telephone number, e-mail addresses, company or VAT number, legal form.

The registrar has the obligation to communicate to DNS Belgium the exact reference of the part of its website where referral is made to the domain name registration. DNS Belgium has the right to record this reference on its own website so that customers can contact the registrar directly. DNS Belgium also has the right to update this reference if it proves to be outdated. The registrar also needs to ensure that the contact details on its website are up-to-date and that it can be contacted by its customers during office hours for technical and administrative support. The registrar shall be free to choose the means of providing such support (e.g. telephone helpdesk, call centre, e-mail, ticketing system, chat function, etc.) on condition that assistance is provided to customers within a reasonable timeframe.

The registrar will also communicate an ‘abuse’ contact address (e-mail address or specific URL) where third parties can report abuse in connection with a specific .be domain name. DNS Belgium will include this ‘abuse’ contact in the Whois information for .be domain names.

13.8 Severability clause

If one or more provisions of this agreement appear to be invalid, unenforceable or illegal, the other provisions remain in full force. DNS Belgium and the registrar also agree to replace the invalid, unenforceable or illegal provision by a valid, enforceable and legal provision preserving the economic aims and maintaining the spirit of the provision so replaced.

13.9 Current contract version

This version of the contract shall replace all agreements concluded previously by and between DNS Belgium and the registrar.

13.10. Authorised signature

The undersigned expressly guarantees that he is duly vested with the authority to sign so as to commit his company or organisation lawfully by means of this agreement.

DNS Belgium shall in any event be able to rely on the fact that the mere signing of this agreement entails full consent with this document on the part of the registrar.

For DNS Belgium	For the registrar
	
Philip Du Bois	(name + title)
General Manager	

Annex 1: Registration, renewal and other fees that apply as of 1 January 2027

Annex 2: Data Processing Annex

Annex 1 to the agreement between DNS Belgium and the registrar

1. The fee for the registration of a domain name is € 6.00 (excl. VAT).
   This fee includes the right to use the domain name for a 1-year period after the registration.

2. The renewal fee for the right of use of a domain name is € 6.00 (excl. VAT).

3. The bulk transfer fee amounts to € 500.00 excl. VAT, per requested transaction in so far the portfolio to be transferred does not amount to more than 2,000 domain names. The fee amounts to € 1,000.00 excl. VAT for portfolios between 2,001 and 5,000 domain names and € 1,500.00 excl. VAT, for portfolios in excess of 5,000 domain names. This does not concern the transfer of a domain name at the holder's request but the (partial) take-over of a portfolio of domain names between registrars.

4. The fee for the re-activation of a domain name that was put in “QUARANTINE” status is € 10.00 (excl. VAT). Domain names in “QUARANTINE” status can be re-activated during a period of 40 days following their deletion by the registrar that had the domain under his management upon the time of the deletion.

5. The fee to transfer a domain name to another registrar amounts to € 6.00, excl. VAT. This fee is only charged insofar as the transfer was successful. After the transfer a new registration period of 1 year commences. There is no reimbursement for the remaining part of the original registration period due to the transfer.

6. The fee for the transfer of a domain name in “QUARANTINE” status before the transfer, amounts to € 10.00, excl. VAT. The successful processing of this type of transfer immediately results in the reactivation of the domain name.

7. The fee for locking a domain name through the activation of the Domain Guard service, amounts to € 80,00 VAT excl. per year. This fee includes 4 temporary deactivations of Domain Guard per year. Extra temporary deactivations during the same year will prompt an additional fee of € 80,00 VAT excl. (including 4 more temporary Domain Guard deactivations).

8. The activation and deactivation of the Domain Shield service is free of charge.

9. The turnover figure to be generated annually by the registrar shall amount to an equivalent of 250 paying domain name transactions. The term ‘paying domain name transaction’ refers to new registrations, renewals executed transfers and reactivations. Each of these transactions shall each time add 1 unit to the actual turn-over figure. In case of a takeover of an existing portfolio by the registrar, the equivalent in units of the total number of domain names that were taken over, will likewise be added to the actual turnover figure.

10. The costs for DNS Belgium for the interventions mentioned in Article 6 (correction of the registrant’s data or deactivation of the transfer lock function) shall amount to €135, exclusive of VAT per file.

Annex 2 to the Agreement by and Between DNS Belgium and the Registrar: Data Processing Annex

WHEREAS:

The registrar has concluded a Registrar Agreement (hereinafter referred to as the Agreement) with DNS Belgium to be able to take part in the registration process of domain names ending with .be;

The registrar can process certain personal data in a processor capacity on behalf of DNS Belgium when registering, renewing, transferring or managing .be domain names;

The registrar and DNS Belgium wish to lay down provisions that shall apply if and to the extent that the registrar acts as a processor on behalf of DNS Belgium.

WHEREFORE, IT IS HEREBY AGREED AS FOLLOWS:

1 Interpretation

1.1 This Data Processing Annex shall be governed by the terms and conditions set out in the Agreement. Capitalized terms that are not defined in this Data Processing Annex shall acquire the meaning given in the Agreement, unless the context indicates otherwise.

1.2 In this Data Processing Annex, the following terms shall mean:

Data Processing Annex: the current data processing annex, including any appendices to this data processing annex;

Third country: as indicated in Article 8;

Services: the services that the registrar provides by virtue or in connection with this Agreement, namely the registration and management of domain names ending with .be in the name of the registrants but for the account of the registrar;

Data Protection Legislation: means any law, enactment, regulation, regulatory policy, by law, ordinance or subordinate legislation relating to the processing, privacy, and use of Personal Data, as applicable to the registrar, DNS Belgium and/or the Services, including:

- the Belgian Act of 30 July 2018 on the protection of natural persons with regard to the processing of personal data; and
- the Regulation of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (**GDPR**), and any corresponding or equivalent national laws or regulations in Belgium;

in each case, as in force and applicable, and as may be amended, supplemented or replaced from time to time;

Approved Subcontractors: contractors including, but not limited to, resellers, who are approved by DNS Belgium in accordance with Article 7.2;

Agreement: the Registrar Agreement as indicated in Recital 1 of this Data Processing Annex;

Personal Data: the personal data that the registrar or any Approved Subcontractors process in a processor capacity on behalf of DNS Belgium in connection with the provision of the Services; "**processing**" of personal data and "**personal data**" shall acquire the meaning given thereto in the Data Protection Legislation.

1.3 DNS Belgium and registrar acknowledge and agree that this Data Processing Annex shall constitute an integral part of the Agreement. If there is a conflict or inconsistency between:

1.3.1 A term from one of the appendices to this Data Processing Annex; and
1.3.2 A term from the main section of this Data Processing Annex; and
1.3.3 A term from the Agreement and its annexes;

The term falling into the category first appearing in the list above shall take precedence.

2 Scope and purpose

2.1 The provisions of this Data Processing Annex shall apply only and to the extent that the registrar processes the Personal Data in a processor capacity on behalf of DNS Belgium.

3 Compliance with the data protection legislation

3.1 The registrar shall comply with its obligations under all applicable Data Protection Legislation at all times when processing Personal Data.

3.2 The registrar shall process Personal Data only:

3.2.1 In the way and for the purposes set out in Article 4; and
3.2.2 According to the instructions of DNS Belgium.

4 Nature and purpose of the processing and processing instructions

4.1 Personal Data shall be processed by the registrar in order to register, renew, transfer and manage .be domain names on the technical platform and network of DNS Belgium.

4.2 DNS Belgium hereby gives:

4.2.1 Instructions to the registrar to take such measures as are reasonably necessary to process Personal Data on behalf of DNS Belgium in order to register, renew, transfer and manage .be domain names on the technical platform and network of DNS Belgium; and
4.2.2 Consent to the registrar to give instructions to the Approved Subcontractors and on behalf of DNS Belgium which are equivalent to the instructions set out in Article 4.2.1.

5 Confidentiality and security

5.1 The registrar undertakes to treat all Personal Data confidentially. Unless required otherwise by DNS Belgium, the registrar shall not disclose any Personal Data to a third party other than:

5.1.1 Its own employees, Approved Subcontractors or employees of the Approved Subcontractors for whom such disclosure is reasonably necessary for the provision of the Services; or
5.1.2 Insofar as required by law, by any government body or other regulatory authority, or by a court or other competent body; and

On condition that the persons to whom Personal Data may be disclosed pursuant to Article 5.1.1. are bound by obligations of confidentiality which correspond with those imposed on the registrar by this Data Processing Annex or by the Agreement;

5.2 Taking into account the state of technology, the execution costs, as well as the nature, scope, context and purposes for processing Personal Data, the registrar shall take appropriate technical and organizational measures to prevent any accidental or unlawful destruction, loss, modification, unauthorised disclosure of or access to the Personal Data. Without limiting the generality of the foregoing, the registrar will (and will ensure that the Approved Subcontractors will) implement the security measures set out in Annex II and will keep these measures in place for the entire term of this Data Processing Annex.

6 Notification of a breach in connection with personal data

6.1 The registrar will provide DNS Belgium with written notice as promptly as reasonably possible upon becoming aware of any actual or potential breach of security that leads (or may lead) to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, any Personal Data (or any media or carrier containing the same) held by the registrar or Approved Subcontractors (such actual or potential breach is hereafter referred to as a "**Data Security Incident**").

6.2 The registrar will (and will ensure that the Approved Subcontractors will) fully cooperate with DNS Belgium, at the registrar's costs and expenses, in handling the Data Security Incident.

7 Subcontracting and subprocessing

7.1 The registrar may outsource all or part of the Personal Data processing to subcontractors (including but not limited to resellers) provided the registrar and the subcontractor have concluded a written processing agreement which imposes obligations that correspond to those stipulated in this Data Processing Annex.

7.2 DNS Belgium hereby gives its consent for the outsourcing of the Personal Data processing pursuant to Article 7.1.

8 Transfers of personal data to third countries

Provisions applicable only if the registrar is established outside the European Economic Area

8.1 When processing Personal Data under or in connection with the Agreement, the registrar shall do so in accordance with:

8.1.1 all applicable Data Protection Legislation; and

8.1.2 the terms set out in Appendix 1 to this Data Processing Annex. For the purpose of this Appendix 1, references to "data importer" shall be deemed to be references to the registrar and references to "data exporter" shall be deemed to be references to DNS Belgium.

Provisions applicable only if the registrar is established in the European Economic Area

8.2 The registrar may transfer Personal Data to a recipient in a country outside the European Economic Area (such a country being referred to as a Third Country), provided that:

8.2.1 The EU Commission has taken an adequacy decision concerning that Third Country in accordance with the applicable Data Protection Legislation;
8.2.2 The recipient participates in a valid cross-border transfer mechanism in respect of which the EU Commission has taken an adequacy decision in accordance with the applicable Data Protection Legislation, so that the registrar (and, where appropriate, DNS Belgium) can ensure that appropriate safeguards are in place to ensure an adequate level of data protection in respect of the transferred Personal Data; or
8.2.3 The recipient has concluded an agreement with DNS Belgium which contains model clauses approved by the EU Commission or by another competent governmental authority in accordance with the applicable Data Protection Legislation.

9 Audit

9.1 The registrar shall provide DNS Belgium with all information that the latter needs to verify that the registrar complies with its obligations under this Data Processing Annex. If DNS Belgium so requests, the registrar shall allow DNS Belgium or an inspector authorized by DNS Belgium to conduct an audit at the registrar to ascertain that the latter complies with its obligations under this Data Processing Annex.

9.2 The registrar shall inform DNS Belgium immediately if, in its opinion, an instruction results in a violation of the Data Protection Legislation.

10 Assistance in handling requests from data subjects

10.1 The registrar shall cooperate with DNS Belgium in:

10.1.1 The handling of requests from data subjects in exercising their rights; and

10.1.2 The performance of a data protection impact assessment in connection with the provision of the Services.

11 Term and termination

11.1 This Data Processing Annex shall enter into force on the date of entry into force of the Agreement and shall remain in force for as long as the registrar provides the Services under the Agreement.

12 Return/destruction of personal data

12.1 Within 30 (thirty) days after the expiry or termination of this Data Processing Annex, the registrar shall:

12.1.1 According to the choice of DNS Belgium:

- Return all Personal Data in the possession or under the control of the registrar as of the date of expiry or termination to DNS Belgium, in a common electronic form at the time; or
- Destroy or remove from the computer systems and files all Personal Data in the possession or under the control of the registrar as of the date of expiry or termination; and

12.1.2 Provide DNS Belgium with a list of Personal Data that the registrar is legally required to keep after the termination or expiry of this Data Processing Annex.

Appendix 1 to the Data Processing Agreement

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) for the transfer of data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8 – Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9 – Clause 9(a), (c), (d) and (e);

(iv) Clause 12 – Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18 – Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7

[intentionally left blank]

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Appendix 2 and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter ‘personal data breach’). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of

processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Appendix 2. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

(a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least one month in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in

substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Appendix 2 the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

(a) The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request)

indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public

authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Belgium.

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of Brussels, Belgium.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

ANNEX I

A. LIST OF PARTIES

Data exporter(s):

DNS Belgium

Role (controller/processor): controller

Data importer(s):

The registrar

Role (controller/processor): processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

The registrants

Categories of personal data transferred

Personal data (e.g. name, email address, home address, telephone number; etc.) of the registrants

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

No sensitive data will be transferred

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

The personal data will be transferred when appropriate for the registrar to register, renew, transfer and manage the registrants' .be domain name(s).

Nature of the processing & Purpose(s) of the data transfer and further processing

The personal data will be transferred if and to the extent appropriate for the registrar to register and manage domain names ending with .be in the name of the registrants but for the account of the registrar (including registering, renewing, transferring and managing the registrars' .be domain name(s).

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

See Article 12 of the Data Processing Annex

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

Autorité de la protection des données - Gegevensbeschermingsautoriteit (APD-GBA)

Rue de la Presse 35 – Drukpersstraat 35

1000 Bruxelles - Brussel

Tel. +32 2 274 48 00

Fax +32 2 274 48 35

Email: contact@apd-gba.be

Websites:

https://www.autoriteprotectiondonnees.be

https://www.gegevensbeschermingsautoriteit.be

Appendix 2 to the Data Processing Annex

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

1. Access control to premises and facilities (physical):

a) registrar will maintain physical security systems at all registrar sites which are used to process Personal Data;

b) physical access control will be implemented for all datacenters. Unauthorized access is prohibited by onsite staff, biometric scanning or security camera monitoring at all times (twenty-four (24) hours per day, seven (7) days per week);

c) registrar will maintain procedures for issuing identification badges to authorized staff and controlling physical access to systems under its control;

d) turnstiles will be integrated with access control readers to control physical access at all sites at all times by requiring staff to present a photo identity card prior to entering a registrar site; and

e) visitors must be pre-approved before coming to registrar sites which are used for to process Personal Data and will be required to present identification, sign a visitor log, and be escorted at all times while on the sites.

2. Access control to systems (virtual):

a) registrar will establish and maintain safeguards against an incident leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or unauthorised access to, Personal Data on its systems which are used to process Personal Data;

b) access will be granted to personnel through documented access request procedures. The employees' managers or other responsible individuals must authorize or validate access before it is given;

c) access controls are enabled at the operating system, database, or application level;

d) administrative access will be restricted to prevent changes to systems or applications; and

e) users will be assigned a single account and prohibited from sharing accounts.

3. Access control to devices and laptops:

registrar will implement and maintain security measures with respect mobile devices and laptops that are used to process Personal Data.

4. **Access control to Personal Data:**

   a) access will be granted only after processing an approved “access control form”, i.e. LAN Logon ID, application access ID, or other similar identification;

   b) unique User IDs and passwords will be issued to the users; and

   c) users, once authenticated, will be authorized for access levels based on their job functions.

5. **Transmission and disclosure control:**

   a) registrar will implement and maintain measures to prevent that Personal Data can be read, copied, modified or removed without authorization during electronic transmission or transport, and to enable to check and establish to which bodies the transfer of Personal Data by means of data transmission facilities is envisaged; and

   b) registrar will maintain technology and processes designed to minimize access for illegitimate processing, including technology for the encryption of Personal Data.

6. **Input control:**

   a) registrar will maintain system and database logs for access to all Personal Data under its control;

   b) all registrar systems must be configured to provide event logging to identify a system compromise, unauthorized access, or any other security violation. Logs must be protected from unauthorized access or modification; and

   c) registrar will maintain input controls on its systems.

7. **Job control:**

   a) registrar will implement procedures to ensure the reliability of its employees and any other person acting under its supervision that may come into contact with, or otherwise have access to and process, those Personal Data, such as requiring a certificate of good conduct or any similar type of certificate prior to commencement of employment;

   b) registrar will implement procedures to ensure that its personnel is aware of its responsibilities under this Data Processing Agreement. registrar will instruct and train any persons it authorizes to have access to Personal Data on the applicable Data Protection Legislation as well as on all relevant security standards and will commit them in written form

to comply with the data secrecy, the applicable Data Protection Legislation and other relevant security standards;

c) registrar will promptly act to revoke access to Personal Data due to termination, a change in job function, or in observance of user inactivity or extended absence; and

d) registrar will have in place a data protection policy and a document retention policy, with which its personnel must comply.

8. Incident management:

a) registrar will implement and maintain an incident management procedure that allows registrar to inform DNS Belgium within the required time frame of any security breach;

b) may a security breach (potentially) affect Personal Data, registrar must notify DNS Belgium in accordance with article 8.6(c) in schedule 1 to the Data Processing Agreement; and

c) the incident management procedure includes periodic evaluation of recurring issues that might indicate a security breach.

9. Availability control:

registrar will protect Personal Data against accidental destruction or loss by ensuring:

a) workstations will be protected by commercial anti-virus and malware prevention software receiving regular definition updates; and

b) upon detection of a virus or malware, registrar will take immediate steps to stop the spread and damage of the virus or malware and to eradicate the virus or malware.

10. Business continuity management:

a) registrar will implement and maintain a business continuity plan that will, inter alia, allow registrar to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical unavailability; and

b) registrar will regularly evaluate this plan.

11. Change management:

a) registrar will implement, maintain a change management procedure; and

b) as part of the change management procedure registrar will evaluate the impact on the security and adapt the measures where needed to maintain the agreed security level.

12. Control of instructions:

registrar will implement and maintain procedures to ensure that Personal Data are processed only in accordance with DNS Belgium's instructions.

13. Separation control:

registrar will implement and maintain procedures to ensure that Personal Data collected for different purposes will be processed separately.

14. Regular testing of security measures:

registrar will frequently test, assess and evaluate the effectiveness of its technical and organisational security measures.