Data Processing Agreement - Digital Data Solutions BV as Processor

Parties:

- Company name , statutory located at Full address and registered at the Chamber of Commerce with number Registration number , hereinafter referred to as “Controller”; and
- Digital Data Solutions BV, statutory located at Plantage Middenlaan 42A in Amsterdam and registered at the Chamber of Commerce with number 75762277, hereinafter referred to as “Processor”;

WHEREAS:

1. The Controller and the Processor have entered into an agreement on 11/11/2026 hereafter the ”Agreement”. In the context of the Agreement, the Processor provides services to the Controller.
2. To provide the services, the Processor processes Personal Data on behalf of the Controller in accordance with this Data Processing Agreement.
3. Parties want to give substance to the processing of Personal Data by the Processor via this Data Processing Agreement;

AGREE TO THE FOLLOWING:

1. Definitions

The terms that are taken from Art. 4 of the General Data Protection Regulation (GDPR) and are used in this Data Processing Agreement have the same meaning. In addition, the following terms have the following meaning:

- Controller: The client of Digital Data Solutions BV to whom this Data Processing Agreement applies
- DDPA: Dutch Data Protection Authority
- GDPR: means Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons regarding the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC
- Data Subjects: means the identifiable or identified natural person(s) whose Personal Data is or are processed
- Parties: Processor and Controller referred to jointly
- Security Incident: Any incident regarding security of Personal Data in cases where Personal Data is lost and/or has and/or could become available to unauthorized parties
- Data Processing Agreement: The present Agreement, applicable between parties including its appendices
- Services: All services that Processor provides to the Controller, as mentioned in this Data Processing Agreement.
- Personal Data means any information which the Processor processes on behalf of the Controller within the framework of this Data Processing Agreement, and which can directly or indirectly identify the Data Subject.
- Processor: Digital Data Solutions BV (CookieFirst)
- Sub-Processor: Means any Processor appointed by or on behalf of the Processor to process Personal Data on behalf of the Controller in connection with this Data Processing Agreement.

2. Obligations of the Processor

i. The Processor acts as a 'Processor' in the sense of the GDPR. This means that the Processor only processes the Personal Data supplied by the Controller on behalf of and for the benefit of the Controller in the context of the execution of the Services and this Data Processing Agreement or in connection with a legal obligation. The Processor will not use the Personal Data for any other purpose or in any other way than for the purpose for which the Personal Data were provided or have become known. Appendix 1 states the details of the Processing of Personal Data.
ii. The Processor will not provide the Personal Data to a Third Party, unless this exchange takes place in the context of the execution of this Data Processing Agreement or when this is necessary to comply with a legal obligation.
iii. The Processor further guarantees that every person acting under its authority will process the Personal Data in accordance with this Data Processing Agreement and the applicable laws, and specifically the GDPR.
iv. At the request of the Controller, the Processor will provide the Controller with information about the (security) measures taken in order to comply with the obligations under the GDPR, this Data Processing Agreement and other instructions from the Controller

3. Security And Confidentiality

i. All Personal Data that are passed on by the Controller to the Processor are classified as confidential and must be treated as such.
ii. The Processor will impose the obligation of secrecy on its personnel and all persons engaged by it.
iii. The Parties keep all Personal Data secret and in no way make them known internally or externally, except insofar as:

    a. Disclosure and/or provision of the Personal Data in the context of the execution of this Data Processing Agreement is necessary.
    b. Any mandatory statutory regulation or judicial decision obliges Parties to disclose and/or provide these Personal Data, whereby the Parties first inform the other Party of this.
    c. Disclosure and/or provision of such Personal Data to a third party shall take place with the prior written consent of the other Party.

iv. In determining the appropriate security measures, the Processor will take into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of Data Subjects posed by the processing.
v. In accordance with the applicable laws and regulations stated in Art. 32 GDPR, the Processor shall take such technical and organizational measures, maintain it and adjust it if necessary, that the Personal Data are appropriately protected against loss, unlawful processing or unlawful access. The Processor shall ensure that the systems used by it (including security software and connections) comply with the applicable legal obligations in connection with the processing of Personal Data.
vi. The Processor shall implement the security measures as listed in Appendix 3, in addition to the minimal appropriate technical and organizational security measures as defined by the competent Data Protection Authority.

4. Control

i. The Controller has the right to have an audit carried out at no later than once a year, with a notice of

two weeks, within regular office hours, at his own expense, by independent experts, which is not a competitor of the Processor or related. The Controller shall reimburse the Processor for any cost or expenses incurred as a result of the audit.

ii. The Processor will provide all reasonable cooperation to an audit. In consultation with the Controller, the Processor will implement the reasonable recommendations without undue delay. The Controller will provide the Processor with a copy of the audit report.

iii. In the event of an investigation by the DDPA or another competent supervisory - or investigative authority, the Processor will provide all reasonable cooperation. The Processor will inform the Controller without undue delay, unless a legal obligation prevents the Processor from doing so.

5. Sub-processor

v. The Controller authorizes the Processor to engage Sub-Processors. The Processor will enter into an agreement with the Sub-Processors it has engaged that is in accordance with the relevant legislation and regulations and this Data Processing Agreement.

vi. The Processor will notify the Controller of the addition or replacement of any Sub-Processor. The Controller shall be given 21 days to object, duly motivated and in writing, after receiving such notification.

vii. In Appendix 2 an overview of all currently appointed Sub-Processors is included. In addition, the Controller may at any time request an up-to-date overview of all appointed Sub-Processors.

6. Security Incidents

i. The Processor informs the Controller without undue delay if a Security Incident occurs regarding the processing of the Personal Data, where the Personal Data is lost and/or has and/or could become available to unauthorized parties.

ii. In the event of a Security Incident, the Processor will take measures, to the best of its abilities, to eliminate and/or minimize the impact of the Security Incident. The Processor will cooperate with the Controller in order to be able to comply with the obligation to report Data breaches to the competent authority and the possible communication to Data Subjects.

iii. The Processor shall provide the Controller with enough information to enable the Controller to comply with the obligations to report the incident to the relevant authorities and to Data Subjects.

iv. Such notification shall contain at least the following information:

   a. The nature of the infringement, the categories and the number of Personal Data records, the categories and the number of Data Subjects, the affected Databases;
   b. The name and contact details of the person where more information can be obtained;
   c. The likely consequences of the infringement; and
   d. Measures taken or proposed to address the infringement.

v. In addition, the Processor will reasonably cooperate in carrying out risk assessments, analysing the cause of the incident or breach, identifying required corrective measures and implementing those measures.

7. Rights of / Requests By Data Subjects

i. If the Processor receives a request or complaint from a Data Subject, such as the ones from Art. 12 to 22 GDPR (request for access, rectification, erasure of Personal Data), then the Processor will forward that request timely to the Controller.

ii. The Processor assures the Controller of all reasonable cooperation to ensure that the Controller can meet its obligations with regard to the rights of Data Subjects within the legal or contractual terms.

8. Transfer Of Personal Data

i. In principle, the Processor only processes the Personal Data of Data Subjects within the confines of the European Economic Area and the countries that have been designated by the European Commission as countries offering an adequate level of protection.
ii. The Processor shall only transfer Personal Data to countries for which no adequacy decision has been taken, if this is in accordance with the requirements of the GDPR. If Personal Data processed under this Data Processing Agreement is transferred to a country with no adequacy decision, the Processor shall ensure that the Personal Data is adequately protected. To achieve this, the Processor shall, unless agreed otherwise, rely on EU approved standard contractual clauses and/or approved Binding Corporate Rules for the transfer of Personal Data. In case the consent of Data Subjects is required, the Controller shall bear the responsibility for acquiring it.

9. Liability and indemnity

i. The Processor is only liable for direct damages suffered by the Controller, that is unequivocally caused by a significant breach of this Data Processing Agreement or legal obligations by the Processor.
ii. If a Party fails to comply with the Data Processing Agreement, this Party is liable for the damage and costs that the other Party suffers as a result or has suffered with due observance of the provisions on liability and compensation in the Data Processing Agreement. The amount of the compensation to be paid by the Party will never be higher than the amount paid by the Controller to the Processor for the provision of services over the period of one year.
iii. The Processor indemnifies the Controller for fines and/or penalties from or on behalf of the DDPA and/or other competent authorities that are imposed on the Controller where it is established that these are attributable to gross negligence, intentional action, or malice by the Processor, considering the limitation mentioned in the first and second section of this provision. To be able to make use of this indemnification, the Controller is obliged to:

    a. Immediately notify the Processor of any investigation or other cause that could lead to a Supervisory Authority’s intention to impose a fine and/or penalties;
    b. Act and communicate in consultation with the Processor towards the authority; and
    c. Reasonably object and/or appeal against imposed fines and/or penalties.

iv. The Controller indemnifies the Processor for fines and/or penalties from or on behalf of the DDPA and/or other competent authorities that are imposed on the Processor and where it is established that these are attributable to violations of the GDPR by the Controller. In order to make use of this indemnification, the Processor is obliged to:

    a. Immediately notify the Controller of any investigation or other cause that could lead to a Supervisory Authority’s intention to impose a fine and/or penalties;
    b. Act and communicate in consultation with the Controller towards the authority; and
    c. Reasonably object and/or appeal against imposed fines and/or penalties.

v. The Processor is not liable for damages or fines and/or penalties that incur from wrong use of the software the Processor provides to the Controller.

10. Duration and Termination

i. This Data Processing Agreement comes into effect on the date of signature. This Data Processing Agreement may be terminated by the end of each month.
ii. If this Data Processing Agreement is terminated or dissolved, Parties must continue to comply with the provisions of this Data Processing Agreement regarding confidentiality, liability, indemnification and all other provisions that are intended by nature to remain applicable between the parties after terminations or dissolution of this Data Processing Agreement.
iii. Upon termination of this Data Processing Agreement, the Processor will, at the request of the Controller, make the Personal Data available to the Controller or to a Third Party appointed by the Controller. The Controller must submit this request to the Processor within four weeks. After termination of this Data Processing Agreement and after the requested transfer of Personal Data, the Processor will destroy the remaining Personal Data.

11. Final provisions

i. The Processor and the Controller will provide each other with all the information required in good time to ensure proper compliance with the applicable privacy laws and regulations.
ii. The Controller guarantees the processing of the Personal Data of the Data Subjects, as referred to in this Data Processing Agreement, is not unlawful and does not violate the rights of others. The Controller indemnifies the Processor against all claims relating to this.
iii. In the event of changes to the Services or regulations that affect the processing of the Personal Data, the Parties will consult on any necessary changes to the Data Processing Agreement. The changes in the text of this Data Processing Agreement can only be agreed to in writing by the authorized representatives of the Parties.
iv. If a part of this Data Processing Agreement is deemed prohibited, void or unenforceable, this does not change the validity of the rest of this Data Processing Agreement. Any invalid provision shall be replaced by a provision that is valid and which interpretation shall be as close as possible to the intent of the invalid provision.
v. In case there is a discrepancy between this Data Processing Agreement and the Agreement and/or Parties' general terms and conditions and/or other contracts or documentation agreed upon by Parties, the provisions in this Data Processing Agreement shall prevail.
vi. This Data Processing Agreement can only be amended in writing.
vii. This Data Processing Agreement replaces all prior Data Processing Agreements between parties.

12. Applicable Law/Competent Court

i. Dutch legislation applies to this Data Processing Agreement. The competent court in Amsterdam has jurisdiction to take note of any disputes arising out of or related to this Data Processing Agreement.

Appendix 1

Details of the Processing of Personal Data:

CookieFirst by Digital Data Solutions BV offers compliance solutions for websites concerning the use of cookies. CookieFirst's software identifies cookies on a website of the Controller and helps website owners to execute cookies only if the correct permission or consent is given. If the Controller decides to make use of CookiesFirst's services, the Controller passes along Personal Data (in the sense of the GDPR) of third parties (Data Subjects) to CookieFirst. The Controller is under an obligation to conclude a Data Processing Agreement with CookieFirst. That is why this Data Processing Agreement applies to services of CookieFirst.

Data Processing in short:

By clicking on our cookie banner the following information will be shared with CookieFirst:

- The website visitor consent status or the withdrawal of consent
- The website visitor anonymized IP address
- Information about the website visitor Browser type
- Information about the website visitor Device type
- Information about the website visitor Operating system
- The date and time the website visitor has visited our website
- The country and region of the visitor

CookieFirst will store cookies and local storage in the visitor browser where the consent status is saved, for proof of consent this information is also shared with CookieFirst. The Personal Data is stored until the request for removal, delete your CookieFirst cookies or until the purpose of the archived Personal Data no longer exists. CookieFirst uses cookies that are necessary to obtain the status of consent under the legal basis of these cookies as mentioned in Article 6.1 lit. c of the GDPR.

---

1 Anonymizing IP addresses by removing the last octet of the address and replacing it with “0”.

2 Saving this data is needed to be able to show the banner in EU countries only and for CCPA-compliance by using GEO-templating

3 ibid, 2

Appendix 2

Sub Processors

The Processor has sub-contracted (part of) the processing of the Personal Data to the following Sub-Processors:

Sub-Processor	Location of processing activities	Purposes of processing
OVH BV, The Netherlands	Germany / France	Providing API for saving consent data. Providing hosting services for the Cookies First website and applications Storage of CDN log data
Artia International S.R.L. (IP-API)	Romania	Used by our API to determine country and region enhancing consent data and provide additional banner configurations based on country/region.
BunnyWay d.o.o., Slovenia	Slovenia	Provider of Content Delivery Network (CDN) ensuring global performance of the cookie banner.

Appendix 3

Technical and Organizational Measures concerning GDPR

This document outlines the technical and organizational measures taken by Digital Data Solutions BV to prevent loss of Personal Data or any form of unlawful processing, regarding Data from the Controller that is being saved to servers of Digital Data Solutions BV by using our software.

Organizational measures in short

- Only engineers who work on the parts of the application that involve the Data about website visitors and consents have access to this Data. Other employees are not able to access, modify, or accidentally delete this Data.
- Employee confidentiality statements and Acceptable Use Policy
- Use of strong passwords.
- All privileged access to production systems should use Multi-Factor Authentication (MFA) if possible and over a secure VPN connection.
- Automated logging of actions related to Personal Data.
- Encryption when sending and storing files containing personal data over SSL.

Data Management Policy

Digital Data Solutions BV classifies Data and information systems in accordance with legal requirements, sensitivity, and business criticality in order to ensure that information is given the appropriate level of protection. Data owners are responsible for identifying any additional requirements for specific Data or exceptions to standard handling requirements. Information systems and applications shall be classified according to the highest classification of Data that they store or process.

Data Classification

To help Digital Data Solutions BV and its employees easily understand requirements associated with different kinds of information, the company has created three classes of Data.

Confidential

Highly sensitive Data requires the highest levels of protection; access is restricted to specific employees or departments, and these records can only be passed to others with approval from the Data owner, or a company executive. Examples include:

- Customer Data
- Personally identifiable information (PII)
- Company financial and banking Data
- Salary, compensation and payroll information
- Strategic plans

- Incident reports
- Risk assessment reports
- Technical vulnerability reports
- Authentication credentials
- Secrets and private keys
- Source code
- Litigation Data

Restricted

Digital Data Solutions BV proprietary information requiring thorough protection; access is restricted to employees with a “need-to-know” based on business requirements. This Data can only be distributed outside the company with approval. This is default for all company information unless stated otherwise. Examples include:

- Internal policies
- Legal documents
- Meeting minutes and internal presentations
- Contracts
- Internal reports
- Internal- and external communication

Public

Documents intended for public consumption which can be freely distributed outside Digital Data Solutions BV. Examples include:

- Marketing materials
- Product descriptions
- Release notes
- External facing policies

Labeling

Confidential Data should be labeled “confidential” whenever paper copies are produced for distribution.

Data Handling

Confidential Data Handling

Confidential Data is subject to the following protection and handling requirements:

- Access for non-pre-approved roles requires documented approval from the Data owner
- Access is restricted to specific employees, roles and/or departments
- Confidential systems shall not allow unauthenticated or anonymous access
- Confidential Customer Data shall not be used or stored in non-production systems/environments
- Confidential Data shall be encrypted in transit over public networks
- Mobile device hard drives containing confidential Data, including laptops, shall be encrypted
- Mobile devices storing or accessing confidential Data shall be protected by a log-on password or

passcode and shall be configured to lock the screen after five (5) minutes of non-use
- Backups shall be encrypted
- Confidential Data shall not be stored on personal phones or devices or removable media including USB drives, CD's, or DVD's
- Paper records shall be labeled "confidential" and securely stored and disposed
- Hard drives and mobile devices used to store confidential information must be securely wiped prior to disposal or physically destroyed
- Transfer of confidential Data to people or entities outside the company shall only be done in accordance with a legal contract or arrangement, and the explicit written permission of management or the Data owner

Restricted Data Handling

Restricted Data is subject to the following protection and handling requirements:

- Access is restricted to users with a need-to-know based on business requirements
- Restricted systems shall not allow unauthenticated or anonymous access
- Transfer of restricted Data to people or entities outside the company or authorized users shall require management approval and shall only be done in accordance with a legal contract or arrangement, or the permission of the Data owner
- Paper records shall be securely stored and disposed
- Hard drives and mobile devices used to store restricted information must be securely wiped prior to disposal or physically destroyed

Public Data Handling

No special protection or handling controls are required for public Data. Public Data may be freely distributed.

Technical measures in short

This part briefly summarises the technical measures taken to ensure the Data is kept private and to prevent loss of Data.

- Consent Data is stored on servers in datacenters of OVH in Frankfurt Germany.
- Databases are encrypted with LUKS at rest.
- All access to databases containing consent Data and client Data is restricted based on IP addresses, secure VPN connections and SSL access.
- The datacenters of OVH have the following certifications:

Datacenter	SOC 1 Type II	SOC 2 Type II	ISO/IEC 27001	PCI-DSS
LIM3	yes	yes	yes	yes
RBX8	yes	yes	Yes	Yes

- We make daily snapshots of the databases with Point in Time recovery
- Our application servers are equipped with firewalls and malware scanners:

- Malware scanner

- Web Application Firewall with Machine Learning Rulesets
- Automated Intrusion Detection and Protection
- Proactive Defense
- DDOS protection

Personal Data security

The Processor will at least take the following security measures:

- Encryption of digital files containing Personal data
- Security of the network connection with Secure Socket Layer (SSL) technology or a similar technology
- Restriction of access to the Personal Data to authorised employees
- Back-ups of the Personal Data to restore them in time in case of physical or technical incidents

Separation of Development, Staging and Production Environments

Development and staging environments shall be strictly segregated from production SaaS environments to reduce the risks of unauthorized access or changes to the operational environment. Confidential production customer Data must not be used in development or test environments without the express approval of the COO.

AS AGREED, AND SIGNED IN DUPLICATE:

X

Signature Certificate

Document name: DPA Netgate Clients

Unique Document ID: 51A938EB7F500E56174905E6273F006C71F95E46

LEGALLY SIGNED USING WPesignature
Build. Track. Sign Contracts.

Timestamp	Audit
15/08/2022 12:48 pm CET	DPA Netgate Clients Uploaded by Tom Van den Bos - tom@cookiefirst.com IP 185.212.171.105
15/08/2022 12:54 pm CET	Legal CF - legal@cookiefirst.com added by Tom Van den Bos - tom@cookiefirst.com as a CC'd Recipient Ip: 45.152.180.174
04/10/2022 12:25 pm CET	Legal CF - legal@cookiefirst.com added by Tom Van den Bos - tom@cookiefirst.com as a CC'd Recipient Ip: 185.212.171.105
04/10/2022 12:32 pm CET	Legal CF - legal@cookiefirst.com added by Tom Van den Bos - tom@cookiefirst.com as a CC'd Recipient Ip: 185.212.171.105
04/10/2022 12:34 pm CET	Legal CF - legal@cookiefirst.com added by Tom Van den Bos - tom@cookiefirst.com as a CC'd Recipient Ip: 185.212.171.105