Data Processing Agreement

This Data Processing Agreement (DPA) forms part of the agreement between PFWeb Solutions, trading as HostBrr, and the customer for HostBrr's hosting services, and governs the processing of personal data on the customer's behalf under Article 28 of the GDPR.

1. Parties and scope

Processor: PFWeb Solutions, trading as HostBrr, Gerdasvej 35, 2600 Glostrup, Denmark, CVR/VAT DK44002698 ("HostBrr").

Controller: the customer who has ordered one or more services from HostBrr, as identified in the customer's account ("the Customer").

1.1 This DPA applies to personal data that the Customer, or the Customer's own users, store or process on HostBrr's services:

- Virtual and dedicated servers (VPS and VDS)
- Shared web hosting (cPanel and DirectAdmin) and reseller hosting
- StorageBox and storage servers
- Backups of these services

1.2 For this data the Customer is the controller and HostBrr is the processor. Where the Customer is itself a processor for a third party, HostBrr acts as its sub-processor, and the Customer is responsible for passing on the relevant obligations.

1.3 This DPA does not cover the personal data HostBrr processes about the Customer as its own client (account, billing, support and abuse handling). HostBrr is the controller for that data, and it is processed under HostBrr's privacy policy at https://hostbrr.com/privacy.html.

1.4 This DPA takes effect when the Customer accepts it, by signing it or by continuing to use the services after it has been made available, and applies for as long as HostBrr processes personal data on the Customer's behalf. A signature is not required for it to apply.

2. Definitions

2.1 "GDPR" means Regulation (EU) 2016/679. "Personal data", "processing", "controller", "processor", "data subject", "personal data breach" and "supervisory authority" have the meanings given in the GDPR.

2.2 "Services" means the hosting services the Customer has ordered from HostBrr. "Agreement" means HostBrr's terms of service together with the Customer's orders.

2.3 "Customer Data" means personal data that the Customer, or anyone using the Customer's services, stores on or transmits through the Services.

2.4 "Sub-processor" means a third party engaged by HostBrr that may process Customer Data in order to provide the Services.

3. Processor obligations

3.1 **Instructions.** HostBrr processes Customer Data only on the Customer's documented instructions. The Agreement, this DPA and the Customer's use and configuration of the Services are the Customer's complete instructions. HostBrr will tell the Customer if it believes an instruction breaks the GDPR. If EU or member state law requires HostBrr to process Customer Data in another way, HostBrr will tell the Customer before doing so, unless that law prohibits this.

3.2 **Unmanaged services.** The Services are provided as infrastructure. HostBrr does not access, view or change the content of Customer Data in the normal course of business. Access happens only where needed to provide the Services, to resolve a support request the Customer has made, to handle abuse or security incidents, or where the law requires it.

3.3 **Confidentiality.** HostBrr ensures that everyone it authorises to process Customer Data is bound by confidentiality, by contract or by law.

3.4 **Security.** HostBrr implements the technical and organisational measures in Annex 2 to protect Customer Data, appropriate to the risk as required by Article 32 of the GDPR. HostBrr may update these measures, provided the overall level of protection is not reduced.

3.5 **Legal requests.** If a public authority asks HostBrr for Customer Data, HostBrr will refer it to the Customer where possible. HostBrr will tell the Customer about the request before disclosing anything, unless the law prohibits this.

4. Customer obligations

4.1 The Customer is responsible for having a lawful basis for the processing, for giving data subjects the information the GDPR requires, and for the accuracy and legality of Customer Data.

4.2 The Customer decides what data is stored on the Services and is responsible for securing its own systems: operating system, applications, accounts, passwords and SSH keys, firewall rules inside its servers, and encryption of data where the Customer requires it.

4.3 The Customer is responsible for its own backups. HostBrr's backup features are an aid, not a guarantee, and StorageBox services are not backed up by HostBrr.

4.4 The Customer chooses the location of each service when ordering. By choosing a location outside the EU or EEA, the Customer instructs HostBrr to process Customer Data in that location (see section 6).

5. Sub-processors

5.1 The Customer gives HostBrr general authorisation to engage sub-processors. The current sub-processors are listed in Annex 3.

5.2 HostBrr will notify the Customer at least 14 days before adding or replacing a sub-processor, by email or by a notice in the client area. The Customer may object on reasonable data protection grounds within that period. If the parties cannot resolve the objection, the Customer may cancel the affected Services and receive a refund of fees paid for the period after the cancellation.

5.3 HostBrr imposes data protection obligations on each sub-processor that are no less protective than those in this DPA, and remains responsible to the Customer for its sub-processors' performance of those obligations.

6. International transfers

6.1 Services ordered in a German location are hosted in data centres in Germany, and Customer Data stored on them stays within the EU or EEA, including HostBrr's backups of these services. The two exceptions are outgoing email from shared hosting and files flagged by the malware scanner, both described in 6.3.

6.2 Services ordered in a USA or Singapore location are hosted in that country at the Customer's choice and on the Customer's instruction. HostBrr covers these transfers with the EU Standard Contractual Clauses (Commission Implementing Decision (EU) 2021/914, module three, processor to processor) agreed with the sub-processor or, for US providers certified under it, with the EU-US Data Privacy Framework. Backups of Singapore shared hosting are stored in the USA with the backup provider listed in Annex 3.

6.3 In every location, outgoing email from shared hosting is sent through the mail relay providers in Annex 3, and files flagged as suspicious by the malware scanner on shared hosting and storage servers may be sent to the scanner's vendor for analysis. These providers are located outside the EU or EEA (USA, Canada and India). HostBrr ensures that each such transfer is covered by an adequacy decision, the Standard Contractual Clauses or another valid safeguard under Chapter V of the GDPR.

7. Personal data breaches

7.1 HostBrr will notify the Customer without undue delay, and where feasible within 48 hours, after becoming aware of a personal data breach affecting Customer Data on HostBrr's infrastructure or at one of its sub-processors.

7.2 The notification will describe, as far as known at the time, the nature of the breach, the categories and approximate number of data subjects and records concerned, the likely consequences, and the measures taken or proposed. Information that is not yet available will be provided as it becomes available.

7.3 HostBrr will take reasonable steps to contain the breach and limit its effects. Notifying supervisory authorities and data subjects remains the Customer's responsibility as controller, with HostBrr's reasonable assistance.

7.4 Incidents caused by the Customer's own systems, software, credentials or configuration inside its services are the Customer's responsibility. HostBrr will inform the Customer if it detects such an incident.

8. Assistance and audits

8.1 **Data subject requests.** The Customer controls the content of its services and can answer most data subject requests itself. If HostBrr receives a request concerning Customer Data, it will refer the data subject to the Customer without answering it, unless the law requires otherwise. HostBrr will reasonably assist the Customer where the Customer cannot fulfil a request itself.

8.2 **Other assistance.** HostBrr will provide reasonable information to help the Customer with data protection impact assessments and prior consultations, as far as these relate to HostBrr's processing.

8.3 **Audits.** HostBrr will make available the information needed to demonstrate compliance with Article 28 of the GDPR, primarily through this DPA and its annexes, and by answering reasonable written questions. Where this is not enough, the Customer may

carry out an audit, or have it carried out by an independent auditor bound by confidentiality, on at least 30 days' written notice, no more than once a year, during normal business hours and without disrupting other customers. Each party bears its own costs.

9. Duration, deletion and return

9.1 This DPA lasts as long as HostBrr processes Customer Data for the Customer.

9.2 The Customer can retrieve its data at any time while a service is active. HostBrr does not keep a separate copy for return after termination, so the Customer should retrieve its data before cancelling a service or letting it expire. This is how the Customer exercises its choice between return and deletion under Article 28(3)(g) of the GDPR.

9.3 When a service is terminated, whether cancelled or not renewed, HostBrr permanently deletes the service's data, including its backups held by HostBrr. For VPS, VDS, StorageBox and storage servers this happens at termination, with no retention period. Shared hosting accounts are also deleted at termination, and the copies remaining in backups expire as described in 9.4. Services suspended for non-payment are cancelled, and their data deleted, if the invoice is not paid within the period stated in the terms of service.

9.4 Copies of a terminated shared hosting account that remain in HostBrr's backups are not restored or otherwise used, and are overwritten in the normal backup rotation no later than 14 days after termination. HostBrr may keep Customer Data longer only where the law requires it.

10. General terms

10.1 Each party's liability under this DPA is subject to the limitations of liability in the Agreement, unless the GDPR requires otherwise.

10.2 If this DPA conflicts with the Agreement on the protection of personal data, this DPA prevails.

10.3 This DPA is governed by Danish law. Disputes are settled by the Danish courts, with the court of HostBrr's registered office as the court of first instance.

10.4 HostBrr may update this DPA to reflect changes in the law or in its services. HostBrr will notify the Customer of material changes at least 14 days before they take effect, by email or by a notice in the client area. If a change reduces the Customer's protection and the Customer objects within that period, the Customer may cancel the affected Services and receive a refund of fees paid for the period after the cancellation.

10.5 HostBrr sends notices under this DPA, including breach and sub-processor notices, to the email address registered on the Customer's account, and the Customer is responsible for keeping that address current. The Customer can contact HostBrr about this DPA and other data protection matters by opening a support ticket in the client area at https://my.hostbrr.com.

Annex 1: Description of the processing

Item	Description
Subject matter	Provision of hosting infrastructure: VPS and VDS servers, shared and reseller web hosting, StorageBox and storage servers, and backups
Nature of processing	Storage, hosting, transmission over HostBrr's network, backup and deletion of Customer Data, and access only as described in section 3.2
Purpose	To provide the Services under the Agreement
Duration	The term of the Services, plus the deletion periods in section 9
Categories of data subjects	Determined by the Customer; typically the Customer's own customers, website visitors, users, employees and contacts
Categories of personal data	Determined by the Customer; any data the Customer stores, for example names, contact details, account data, email content, files and log data
Special categories	Not intended. If the Customer stores special categories of data (Article 9 GDPR), it is responsible for appropriate additional safeguards, such as encryption
Locations	The data centre location the Customer chooses when ordering: Germany, USA or Singapore

Annex 2: Technical and organisational measures

Area	Measures
Physical security	Servers are housed in professionally operated data centres with access control, video surveillance, fire protection and redundant power and cooling, run by the data centre providers in Annex 3
Access control	Administrative access to servers only by authorised staff, using SSH keys rather than passwords, from restricted networks; administrative panels protected by individual accounts
Separation	Virtual servers are isolated from each other by KVM virtualisation. Shared hosting accounts are isolated with CloudLinux CageFS and jailed shells, with per-account resource limits
Network and application security	Web application firewall (ModSecurity) and malware scanning (cPGuard / Imunify360) on shared hosting and storage servers; DDoS protection on the network; outbound mail (port 25) blocked on VPS by default and opened only on request
Availability and resilience	RAID storage on servers; daily backups of shared hosting accounts kept for 14 days; optional VPS backup slots; monitoring of servers and services around the clock
Encryption	VPS backups are encrypted at rest. Access to the client area, control panels and webmail uses TLS. Encryption of data inside a service is the Customer's choice
Deletion	Data of terminated services is deleted, including backups held by HostBrr (section 9)
Incident handling	Abuse and security reports are handled through a dedicated Abuse Department, and compromised services can be suspended to contain an incident

Area	Measures
Organisational	Staff with access are bound by confidentiality; access is limited to what each role needs; security updates are applied to HostBrr's systems on a regular basis

Annex 3: Sub-processors

Sub-processor	Service	Location	Customer Data involved
Dataforest GmbH	Data centre for German VPS, VDS, StorageBox and storage servers, and for HostBrr's own backup servers for German shared hosting	Germany (EU)	All data on these services, and backups of shared hosting accounts in Germany
IP-Projects GmbH & Co. KG	Data centre for German VPS, VDS and StorageBox	Germany (EU)	All data on these services
Hetzner Online GmbH	Data centre and servers for part of the German shared hosting	Germany (EU)	All data on these services
InterServer, Inc.	Data centre and servers for USA DirectAdmin hosting, and storage of backups of USA and Singapore shared hosting	USA	All data on these services and their backups
GorillaServers, Inc.	Data centre and servers for USA StorageBox	USA	All data on StorageBox services in the USA
Host Department NJ, LLC	Data centre and servers for USA cPanel hosting	USA	All data on these services
OVH Singapore Pte. Ltd.	Dedicated servers for Singapore hosting	Singapore	All data on services in Singapore
InterServer, Inc. (MailBaby)	Outbound email relay for shared hosting	USA	Outgoing email of shared hosting accounts

Sub-processor	Service	Location	Customer Data involved
MailChannels Corporation	Failover outbound email relay for shared hosting	USA / Canada	Outgoing email of shared hosting accounts, when used
Cloud Linux Software, Inc. (Imunify360)	Malware analysis; may receive suspicious files from shared hosting and storage servers	USA	Suspicious files flagged by the malware scanner
OPSSHIELD LLP (cPGuard)	Malware analysis; may receive suspicious files from shared hosting and storage servers	India	Suspicious files flagged by the malware scanner

HostBrr operates its network in Germany on its own autonomous system (ASN). The IP address space it uses there is leased from GHOSTnet GmbH, which does not process Customer Data.

Payment providers (Stripe, PayPal) and HostBrr's billing, support and monitoring tools process data about the Customer as HostBrr's client, not Customer Data, and are therefore covered by HostBrr's privacy policy rather than this DPA.

Signatures

Signing is optional. Under section 1.4 this DPA also applies when the Customer accepts it by continuing to use the Services.

	Processor	Customer (Controller)
Company	PFWeb Solutions, trading as HostBrr	
Name	Philip Fjærå	
Title	Owner	
Date		
Signature		