Data Processing Agreement

Last updated: September, 2021

1. Introduction

1.1 This Data Processing Agreement ("**DPA**") is an addendum to the General Service Terms entered into between the Customer and DNV (“**Service Terms**”). This DPA supersedes any prior agreement and provision between the parties concerning the processing of personal data.

1.2 This DPA governs any processing of personal data by DNV with respect to the provision of Services where DNV acts as processor on behalf of the Customer as controller, as identified in Annex 1. This DPA does not apply to (i) Services where DNV does not process personal data, (ii) DNV's processing of personal data as controller, including processing of personal data about login details and metadata of the Users' use of any Services, or (iii) where the Customer is not established in the EEA or otherwise not subject to the EU General Data Protection Regulation 2016/679 ("**GDPR**")

1.3 Words and expressions used in this DPA shall have the meaning as defined in the Service Terms, or as defined in applicable data protection law ("**Applicable Data Protection Law**").

1.4 DNV has appointed Aimilia Evdaimon, GDPR responsible Digital Solutions, as a contact person for data protection purposes, available via e-mail: Aimilia.Evdaimon@dnv.com.

2. Customer's obligations

2.1 The Customer shall comply with its obligations as controller under Applicable Data Protection Law, including by:

a) ensuring lawfulness of processing pursuant to GDPR article 6 and 9;

b) exercising the data subjects' rights pursuant to GDPR chapter III;

c) making any required notifications in the event of a personal data breach pursuant to GDPR article 33 and 34; and

d) otherwise complying with its obligations under this DPA.

3. DNV's obligations

3.1 DNV shall as processor:

a) process the personal data as instructed by the Customer, i.e. only for the purpose and within the scope set out in Annex 1 to this DPA, or as otherwise required by applicable law in an EEA member state provided that DNV informs the Customer of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;

b) notwithstanding clause 3.1a), be entitled to anonymize the personal data and to process and disclose such anonymous data for any purpose;

c) taking into account the nature of the processing, assist the Customer by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Customer's obligation to respond to requests for exercising the data subject’s rights laid down in GDPR chapter III;

d) assist the Customer in ensuring compliance with the Customer's obligations pursuant to GDPR articles 32 to 36 taking into account the nature of processing and the information available to DNV;

e) inform the Customer if, in its opinion, an instruction by the Customer infringes Applicable Data Protection Law; and

f) otherwise comply with its obligations under this DPA.

3.2 DNV is entitled to charge a reasonable fee for assistance performed pursuant to clause 3.1 c) and d).

4. Security and data breaches

4.1 DNV shall maintain appropriate technical and organizational measures for the purpose of ensuring a level of security appropriate to the risk. The Customer acknowledges and agrees that the measures described in Annex 2 and/or referred to in Annex 1 are deemed appropriate, and that the security measures may be continuously amended provided that the amendments do not materially reduce the level of data security.

4.2 DNV shall ensure that personnel that have access to personal data are subject to an obligation of confidentiality.

4.3 Notwithstanding clause **Error! Reference source not found.**, the Customer acknowledges and agrees that no systems or services are completely secure, and that personal data breaches may occur.

4.4 In the event of a personal data breach, DNV shall without undue delay notify the Customer in writing. Such notification shall, to the extent DNV has or may reasonably obtain the information, contain information needed by the Customer to comply with its obligations under GDPR article 33 and 34.

5. Sub-processors

5.1 The Customer authorizes DNV to en5gage sub-processors. Sub-processing shall be done by way of a written agreement with the sub-processor that imposes appropriate data protection obligations. Where the sub-processor is engaged for carrying out specific processing activities on behalf of the Customer (which is generally not the case), DNV shall by way of a written agreement impose on the sub-processor the same data protection obligations as set out in this DPA. DNV remains fully liable to the Customer for the performance of the sub-processors' obligations.

5.2 The current sub-processors are listed in Annex 1. DNV shall notify the Customer of any intended changes concerning the addition or replacement of sub-processors and allow the Customer to object to such changes. If the Customer does not object within 14 days from receipt of notice, the changes are deemed accepted. If the Customer objects, DNV may choose to continue the Service without the change or to terminate the Service.

6. International data transfer

6.1 The Customer instructs DNV to only transfer personal data to a third country if the transfer complies with the requirements of GDPR chapter V. The Customer acknowledges and agrees that use of sub-processors pursuant to clause **Error! Reference source not found.** may involve transfer of personal data to a third country if Annex 1 indicates that the address or processing location of such sub-processor is in a third country. In the event of a data transfer to a third country, the EU Standard Contractual Clauses set out in Annex 3 shall apply with respect to such transfer.

6.2 DNV shall, to the extent legally permitted under applicable law, without undue delay notify the Customer if DNV, or a sub-processor, receives a legally binding request from a supervisory authority in a third country to disclose personal data processed under this DPA or if DNV becomes aware of any direct access by public authorities to personal data processed under this DPA, and DNV shall, and shall procure that any relevant sub-processor shall, prevent or limit disclosure of or access to such personal data to the extent reasonably possible. If DNV, or the relevant sub-processor, is prohibited under applicable law from notifying the Customer, DNV, or the relevant sub-processor, shall use reasonable endeavors to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible.

7. Audits

7.1 DNV shall maintain necessary records and upon request, make available to the Customer the information necessary to demonstrate compliance with this DPA and Applicable Data Protection Law.

7.2 DNV shall allow for and contribute to audits by the Customer through an independent auditor which is not a direct competitor of DNV, subject to adequate confidentiality undertakings. Audits shall primarily be performed by requesting DNV to submit internal or third party audit reports concerning the processing operations subject to this DPA.

7.3 If the Customer substantiates a legitimate reason do to so, it may request on-site audit. Such request shall to the extent possible be given in writing at least 14 days in advance. On-site audits cannot be requested more than once per year, unless the Customer substantiates a legitimate reason to do so more often. On-site audits shall to the extent possible be conducted within ordinary working hours and seek to avoid obstruction of DNV's activities. DNV may on a case-by-case basis stipulate other reasonable conditions for the on-site audit. DNV shall receive a copy of any audit reports produced by or on behalf of the Customer.

7.4 Each party shall bear their own costs in relation to audits requested by the Customer.

8. Liability

8.1 Unless otherwise follows from mandatory law or the Standard Contractual Clauses, the provisions of *no warranties*, *limitation of liability* and *indemnity* as set out in the Service Terms apply correspondingly to this DPA, and the Customer acknowledges and agrees that if a supervisory authority imposes a fine on the Customer, DNV has no responsibility for reimbursing such fine.

9. Term and termination

9.1 This DPA will remain in force as long as the Service Terms are in effect for the Service for which personal data is processed.

9.2 Upon expiry or termination, DNV shall, at the choice of the Customer, return (including by allowing the Customer to itself extract data from the Service) or delete the personal data. DNV may however continue to store the personal data to the extent required by applicable law in an EEA state, and DNV may in any event retain its backup according to its backup routines, provided that DNV will not actively process such personal data.

Annex 1 – Nature, purpose and subject matter of the processing of personal data

Service #1	**Phast Online**
Purpose	The purpose of the processing of personal data is to provide the Service.
Categories of data subjects	Any data subject(s) the Customer decides to share a workspace with.
Categories of personal data	Names and e-mail addresses of the data subjects whom the Customer shares a workspace with.
Sub-processors	N/A
Special provisions	For the avoidance of doubt, as between DNV as processor and the Customer as controller, the Customer is solely responsible for any controller and processing relationships with its data sources, other processors, customers and other third parties.

Annex 2 – Technical and organizational security measures

This text reflects the security responsibilities for DNV as a service provider to the DNV Business Areas and customers. Our service offerings are built using different platforms.

GENERAL INFORMATION

DNV is ISO27001 certified which covers information security and security of personal data (with exception of business assurance certification services). The purpose of the information security management system is to establish and maintain appropriate processes and adequate risk assessments and controls, including technical measures like encryption, anonymization and secure communication.

PHYSICAL ASSET MANAGEMENT ON PREMISE

DNV only allows hardware to connect to the internal network that has been subject to DNV approval, and that has been recorded in the internal IT register. The asset registration includes information such as a unique description, the specific business purpose, the physical location of the asset, and applicable compliance requirements. The asset is tracked throughout its lifecycle to endeavour that all assets are accounted for, and that no assets unable to meet the criteria of the approval are connected to the internal IT network.

APPLICATION SECURITY

All network traffic within our solutions are encrypted using standard secure transport protocols. Certificates and keys are stored securely. Multiple encryption methods, protocols, and algorithms are deployed to help provide a secure path for data to travel through the infrastructure - Protocols and technologies examples include: Transport Layer Security/Secure Sockets Layer (TLS/SSL), symmetric cryptography based on a shared secret to encrypt communications as they travel over the network.

ACCESS CONTROL

All users are identified by User ID, authenticated by DNV identity management systems. Authorization of users to different services or datasets are managed on instructions from the data owner / service owner. All DNV user accounts are protected by user ID and password and reviewed regularly. Successful and unsuccessful sign-on attempts are logged, and dormant DNV accounts are removed

SYSTEM MANAGEMENT

DNV considers security architecture principles, business objectives and security requirements, with security metrics defined and monitored. All Servers and Cloud subscriptions are registered in an asset register and are running with approved set-up and configured in accordance with approved IT System documentation. Servers and Cloud services are monitored and reviewed regularly by authorized personnel.

DNV monitors the performance and availability of the services. Backup is performed according to obligations set out in applicable agreements.

Disaster recovery plans are implemented and tested on regular basis with dry runs.

NETWORKS & COMMUNICATION

Network Devices are configured, implemented, and documented, with respect to access, vulnerability, patch management, routing tables and settings, including logging of security-related events for review. All business-critical network devices are monitored by authorized personnel to endeavor preventing attacks and failures.

TECHNICAL SECURITY MANAGEMENT

All servers and client PCs running Windows, Linux, Unix operating systems have approved and updated software for protection from malicious code being installed, and this protection is active always. All systems are required to have the minimum-security controls e.g. Anti-malware virus, Firewalls, and Intrusion detection and prevention.

THREAT & INCIDENT MANAGEMENT

Security Incident Management is an extension of the normal incident management process. When security incidents occur, the security incident team provides reasonable co-ordination, management, feedback and communication. They will also assess, respond to, and learn from information security incidents to understand the risk and reduce the risk of reoccurrence.

Information on the current threats and vulnerabilities is important to understand where security improvement measures should be prioritized.
Security-related event logging is enabled on relevant services. Security log files are protected for the purpose of avoiding unauthorized access and modifications, and methodically and continuously analyzed.

LOCAL ENVIRONMENT MANAGEMENT

Local environment management of the IT system landscape defines the requirements for physical protection against accidents, attacks, power outage and unauthorized physical access.
The IT system landscape is implemented in global data centres, as well as many facilities with extended set-up and asic set-up. It is defined to reflect industry best practices and recommendations from relevant standards (such as TIA-942), and contains detailed requirements to facilities, including fire and water detection, fire extinguishers, rack, cabling and power, electricity and cooling, and secure network connections.

RECOVERY OF IT SERVICES

IT recovery plans for IT systems are established in agreement with users and stakeholders, with defined Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) for individual systems and services. These plans include arrangements for resuming IT services by using alternative facilities and covers scenarios where single or multiple facilities (global data centres, extended and basic set-up facilities) are inoperative.

DATA ENCRYPTION

Encryption serves as the last and strongest line of defense in a multi-layered data security strategy, and employ multiple encryption tools, technologies, methods, protocols and algorithms across products and services to help provide a secure path for data to travel through the infrastructure, and to help protect the confidentiality of data that is stored within the infrastructure.

SUB-PROCESSOR'S SECURITY MEASURES

To the extent DNV uses sub-processors in its provision of the Service (as set out in Annex 1), the at all times applicable technical and organizational security measures of such sub-processor will supplement the measures described in this Annex 2. Information regarding such measures by the sub-processor may be found on the sub-processor's website, or by contacting such sub-processor directly.