Appendix 4.2 Special Terms & Conditions

SUPPLEMENTARY DEFINITIONS

Term	Definition
Acceptable Use Policy	means the acceptable use policy which applies to a particular cloud service product provided under the Call-Off Contract. The Acceptable Use Policy is deemed a part of the Supplier's General Terms & Conditions.
CCM-CSA	means "Cloud Controls Matrix – Cloud Security Alliance", a cybersecurity control framework for cloud computing.
C5	stands for "Cloud Computing Compliance Controls Catalog", a set of security controls and regulations developed by the German Federal Office for Information Security (BSI) that defines the baseline for cloud security.
Customer Authorised Representative	means a person authorised to represent the Customer in the execution of the Call-Off Contract. The Customer Authorised Representative at the Effective Date is described in the Order Form.
Customer's Existing Entitlement	means Customer's funds held on account by the Supplier in respect of another transaction(s) outside of this Contract and to be used as part or whole payment of the Charges.
CWE/SANS Top 25	""Common Weakness Enumeration" / SANSTop 25 represent a listing of the 25 most common and impactful software weaknesses.The list is updated annualy.
Data Subjects	shall have the meaning defined under GDPR Art. 4
FedRAMP	means "The Federal Risk and Authorization Management Program". As defined by the U.S. General Services Administration, it is "a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services."
IETF RFC 7643	means Internet Engineering Task Force Request for Comment 7643 System for Cross-domain Identity Management, focusing on cloud-based applications and services.
Minimum Commitment	shall have the meaning ascribed to such term in clause 4.4 of Appendix 2 (*Charges*),
Open-Source Software	means software licensed under a freeware, shareware or any similar free or open-source software license.
OWASP ASVS	stands for "Open Worldwide Application Security Verification Standard Project", an international non-profit organization dedicated to improving the security of software.
Personal Data	shall have the meaning as defined under GDPR Art. 4
SCIM 2.0	means "System for Cross-domain Identity Management 2.0"
Security incident	means the same as defined in the EU NIS2 directive: "an event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems."
Services	means the services delivered under this Framework Agreement, including the Platform.
Service Level Agreement	means the Supplier's relevant service level terms and conditions which apply to a particular cloud service product provided as part of the Services under this Contract.
Service Request	means a request for additional services submitted by or on behalf of the Customer.

Service Terms	means the relevant part of Supplier Standard Terms & Conditions, which apply to a particular cloud service product provided under the Call-Off Contract.
SOC2 Type 2	means "Service Organisation Control 2 Type 2", an auditing procedure that ensures and documents that a service provider securely manages data to protect the interests of the organization and the privacy of its clients.
Supplier Authorised Representative	means a person authorised to represent the Supplier in the execution of the Call-Off Contract. The Supplier Authorised Representative at the Effective Date is described in the Order Form,
Platform	means the technical solution/platform provided by the Supplier where the Customer may utilise the Services made available on the technical solution/platform.
Third Party Software	means any application, component or software not incorporated in the Services and provided by a third party under direct license terms.

SECTION A: SERVICE TERMS

1. INTRODUCTION

The Supplier shall while performing under the Call-Off Contract comply with all requirements set out in this Appendix 4.2 (*Special Terms & Conditions*). Appendix 4.2 (*Special Terms & Conditions*) supplements Appendix 4.1 (*General terms & Conditions*).

2. THE SERVICES

2.1 The Supplier shall provide the Services under the Call-Off Contract at least in accordance with;

a) best industry practice and with high professionalism;

b) all relevant practices and standards for delivering services that are identical or similar to the Services; and

c) any applicable service levels.

2.2 The Supplier shall ensure and document upon Customer's request that the personnel performing Professional Services:

a) possess the required formal education, expertise and experience required to perform the tasks they have been allocated to.

b) have received and will maintain necessary and relevant knowledge of the Customer, its business, products, processes, applications, systems and relevant Laws.

c) have received sufficient instructions as to the contents of the Call-Off Contract, the Services and the service levels associated therewith; and

d) possess required and appropriate language skills.

2.3 Service Requests

2.3.1 The Customer may throughout the Call-Off Contract term order additions to their licenses, as set out in Appendix 2 (*Charges*) ("Service Requests"). Service Requests shall be responded to as soon as possible and will take effect immediately from the time of activation.

2.3.2 Service Requests must be submitted by an authorised representative of the Customer.

2.3.3 The Customer is entitled to exercise any flexibility as provided for in the Call-Off Contract and as otherwise offered by the Supplier as an enhanced flexibility relating to the Service in question, including rights to increase / decrease the volume of Services, make changes to type and quantity of Services etc.

3. MODIFICATION AND CHANGES TO THE SERVICES

3.1 General

3.1.1 Any changes to the Services are subject to written agreement between the Parties in accordance with clause 10.1 a) of Appendix 4.1 (*General Terms & Conditions*) except as provided for in clause 2.3 above and this clause 3.

3.1.2 The Supplier shall continuously improve and develop the Services, and grant Customer access to new functionality throughout the Call-Off Contract.

3.2 Log of modifications

3.2.1 Full details of all changes, updates and modification to the Services ("Service Modification") shall be maintained in a log that is available for review by Customer.

3.3 Modification and changes without prior written notice

3.3.1 The Supplier is not required to provide prior written notice of Service Modifications in accordance with clause 3.4 where the Service Modification enhance functionality, security or performance provided that:

a) the modification does not remove or diminish any part of the Service utilised by any Customer e.g., a reduction of functionality and/or service, and/or loss of compatibility with any third-party supported operating systems used by the Customer; and

b) applies on a uniform basis to all the Supplier's customers in respect of the affected Services.

3.3.2 The Supplier is not required to provide prior written notice of Service Modifications in accordance with clause 3.4 where Service Modifications are reasonably necessary to:

a) comply with Law and such requirement to comply is imminent and was reasonably unforeseen by the Supplier in the circumstances; or

b) maintain the security of the Supplier's technology infrastructure

(in each case an "Urgent Service Modification"). If the Urgent Service Modification entails changes that the Supplier should have notified pursuant to clause 3.4 prior to performing the modification, the Supplier shall as soon as is reasonably possible provide the Customer Authorised Representative a written notice of the date on which such Urgent Service Modification was made, including a brief summary with details, and such information as set out in clause3.4.4.

3.3.3 If the Customer becomes aware of a service modification performed without prior written notice, that, in the Customer's opinion, should have been notified in accordance with clause

3.4 prior to performing the modification, clause 3.4.5 and 3.4.6 apply mutatis mutandis from the time the Customer was made aware of the Service Modification.

3.4 Modifications and changes with prior written notice

3.4.1 The Supplier shall notify the Customer in writing as soon as possible prior to any Service Modification taking effect provided that:

a) The Service Modification requires the Customer to modify their usage of the Services, including, but not limited to, configuration, set-up, integration, or the Service Modification discontinues, removes, reduces or diminishes the Services; and

b) applies on a uniform basis to all the Supplier's customers in respect of the affected Services.

3.4.2 For discontinuation of Services, the Supplier shall notify as soon as possible, and no later than 90 days prior to the Service Modification taking effect.

3.4.3 For other Service Modification with a notification obligation, the Supplier shall notify as soon as possible, and no later than 60 days prior to the Service Modification taking effect.

3.4.4 The Notification shall include information setting out in full and in a clear manner the Service Modification, or a hyperlink directly to a URL where information about the Service Modification, consequences and effective date is set out in a clear manner.

3.4.5 The Customer may object to the proposed modification or update by notifying the Supplier withing 45 days in which case the Parties shall immediately, acting reasonably, attempt to resolve the Customer's objection. If the Parties are not able to agree on a solution satisfactory for the Customer within 30 days before the planned effective date of the proposed modification or update, the matter shall be escalated to DFØ for further good faith negotiations.

3.4.6 If the Parties are not able to agree on the change according to 3.4.5**Feil! Fant ikke referansekilden.** above, and the Supplier anyhow makes the change effective on the Services, the Customer shall have the right to:

a) terminate the Call-Off Contract, or relevant Services under a Call-Off Contract, with immediate effect and without any liability as long as the Service Modification entails a discontinuation of a Service useful to the Customer, or the Service Modification significantly reduces the Customer's effect of the usage of the Services.

3.5 Application programming interfaces (APIs)

3.5.1 In the event a proposed modification or update related to an API affects the Customers usage of the API:

a) The Supplier shall notify the Customer in writing at least 30 days prior to the planned effective date of such changes; and

b) the previous API shall continue to be made available for use by the Customer for a period of at least 90 days following the modification or update to the API.

3.5.2 Any modification, update or change to an API that are already in use by the Customer shall be made available to the Customer free of charge. This includes where the Supplier implements a new API as a substitute for a previous API.

3.5.3 Clause 3.5.1 does not apply to security patching of APIs performed in accordance with clauses 16.2.116.2

4. ACCEPTABLE USE POLICY

4.1 The applicable Acceptable Use Policy shall be set out in Appendix 4.5 (*Supplier Standard Terms & Conditions*).

5. SERVICE TERMS

5.1 The applicable Service Terms that apply to the Call-Off Contract shall be set out Appendix 4.5 (*Supplier Standard Terms & Conditions*).

6. THIRD PARTY SOFTWARE

6.1 The Supplier shall ensure assurance of license compliance with all third party software vendors used as part of the service, as well as compliance with information security requirements, cf. clause 14.514.5 and the requirements to Data Protection set out in clause 21.

7. OPEN SOURCE

7.1 The Supplier shall ensure assurance of license compliance with all open source software and data sources used as part of the service, as well as compliance with information security requirements, cf. clause 14.5 and the requirements to Data Protection set out in clause 21.

7.2 The Supplier shall inform if there are certain limitations or consequences for the Customer regarding the use of the Services due to the usage of Open Source Software licensing.

8. HYPERLINKS

8.1 The Supplier may use hyperlinks as a reference to their terms and conditions. Each hyperlink shall be directly to a URL setting out in full and in a clear and transparent manner applicable terms and conditions. The Supplier shall make clear towards the Customer if their terms and conditions consists of several documents referenced to by several Hyperlinks and URLs.

8.2 The Supplier shall offer a list of all relevant Hyperlinks, as well as a introduction guide as to the relevant documents and where to find the necessary information applicable for the Customer.

9. CHARGES AND INVOICING

9.1 Charges

9.1.1 The Charges are regulated in the Framework Agreement's Appendix 2 (*Charges*).

9.2 Invoicing

9.2.1 The Supplier shall invoice the Customer in accordance with the Order Form. The invoices shall be specified and documented in order for the Customer to easily check whether the invoice conforms to the agreed consideration. Disbursements shall be specified separately.

9.2.2 The Supplier shall use electronic invoices in an approved standard format in accordance with regulations of 2 April 2019 on electronic invoices in public procurement. The Supplier shall bear any costs associated with electronic invoicing.

9.2.3 In the event of non-payment in whole or part of any sum due by either Party to the other under the Call-Off Contract within 30 (thirty) days of the due date for payment thereof, the Party to whom the payment is due shall be entitled to charge interest on the outstanding sum unpaid from the due date until the actual date of payment (as well after as before decree or judgment) pursuant to the Norwegian Late Payments Interest Act.

9.2.4 If there's an invoice dispute, the Customer must pay any undisputed amount and return the invoice within 30 (thirty) days of the invoice date. The Customer will provide a covering statement with proposed amendments and the reason for any non-payment. The Supplier must notify the Customer within 10 (ten) days of receipt of the returned invoice if it accepts the amendments. If it does, then the Supplier shall provide a replacement valid invoice with the response.

9.2.5 The payment of any amount pursuant to an invoice shall not prevent the Customer raising a dispute in respect of that amount and shall not in itself constitute acceptance by the Customer as to the performance by the Supplier of any of its obligations under the Call-Off Contract.

9.3 Customer's right to setoff

9.3.1 The Customer may set off any amount owed to it by the Supplier (irrespective of whether the amounted relates to the respective Call-Off Contract) against any amount due to the Supplier.

9.3.2 The Supplier has no right to make setoff against any amount due to the Customer.

10. SERVICE LEVEL AGREEMENT

10.1 For each service product provided, the Supplier's relevant service level terms and conditions shall apply to the Services. Breach of applicable service level shall be compensated in accordance with the Supplier's Service Level Agreement with an increase of 20 %.

10.2 The following failures to the SLA shall constitute a material breach entitling the Customer to terminate the applicable Call-Off Contract:

a) 1 (one) failure to the service level, where the service level is below 90 % through the calculation period;

b) a) 2 (two) consecutive failures; or

c) 3 (three) failures to the same service level in any rolling 6 (six) month period

10.3 The applicable service level agreement shall be included or referred to in Appendix 4.5 (*Supplier Standard Terms & Conditions*) in sufficient details so that the Customer can easily understand when service credits will accrue.

10.4 The Supplier shall as soon as possible notify the Customer if the Services do not perform or are likely not to perform in accordance with the applicable service level.

10.5 The fee for breach of the service level shall automatically be made available for the Customer the following month, without the need of the Customer to submit a claim for such breach. The Service Credits shall be reimbursed to the Customer as soon as possible, or may be set off against accrued services.

10.6 The fee is an adjustment of the relevant Charges and is not an estimate of the loss or damage that may be suffered by the Customer as a result of the Supplier's failure to meet service levels and is without prejudice to any other rights or remedies of the Customer arising from the Supplier's failure to meet any service level.

11. TERMINATION FOR CONVENIENCE

11.1 In addition to the termination rights under the Supplier Standard Terms & Conditions or as otherwise offered by Supplier in general, the Customers may terminate any Call-Off Contract fully or partially (including 1 (one) or several individual Services or parts of individual Services) for convenience with 30 days without any termination fee or other compensation to the Supplier.

11.2 In addition, the Customer may terminate any Call-Off Contract fully or partially without additional liability for any Parties and with immediate effect:

a) if the Supplier becomes or is, in the reasonable opinion of the Customer, likely to become subject to a Change of Control situation if, in the reasonable opinion of the Customer, such Change of Control situation has (or shall have) a material adverse effect on the suitability and capacity of the Supplier following such Change of Control to fulfil its obligations under the Call-Off Contract or for a specific Service under the Call-Off Contract (such assessment of suitability to include, without limitation, consideration of the financial standing, nationality/origin, internal safety considerations and historic ethical behaviour);

b) if the Customer, in its reasonable opinion, considers the purchase or use of the Service to be in breach of applicable Laws;

c) the Framework Agreement is terminated before expiry, for any reason;

d) if the Customer becomes subject to the Norwegian Security Act or similar legislation; or

e) if a competent governmental body recommends termination based on consideration relating to the Norwegian Security Act or similar legislation.

11.3 Customer's right to terminate for convenience shall be without prejudice to any other rights or remedies of the Customer. If Customer terminates for cause, and the termination is later proved unjustified, Customers maximum liability for damage shall not be higher than as if Customer had exercised its right to terminate for convenience.

11.4 The Supplier is not obliged to refund any pre-paid revenue for the Services when the Customer exercises its right to terminate for convenience.

12. EXIT

12.1 In the event of expiry or termination of the Call-Off Contract, for any reason, the Supplier shall retain the Customer Data and allow the Customer to extract the Customer Data for a period of 30 days following expiry or termination. The Supplier shall be entitled to a reasonable charge for continuing to provide the Customer with access to the Services for this purpose during the relevant period.

12.2 The Supplier shall enable the orderly and efficient migration of Customer Data to the Customer and/or the replacement supplier. Upon request of the Customer, this shall also include:

a) providing the Customer and/or the replacement contractor with all necessary information; and

b) cooperate with the Customer and/or the replacement contractor with the transfer of all Customer Data.

12.3 Except in circumstances where the Call-Off Contract is terminated pursuant to clause 12.2.1 of Appendix 4.1 (*General Terms & Conditions*), the Supplier may request a reasonable fee for providing exit services which cannot be higher than a fee on a time & material basis based on Supplier's standard rates (or, if lower, any agreed hourly rates forming a part of the Charges).

12.4 The Supplier shall ensure that all Customer Data will be deleted following termination and the completion of the exit, and provide a written declaration of such deletion, including a specification of the method of destruction to the Customer upon request.

13. DOCUMENTATION

13.1 Documentation referred to in this appendix and/or any Data Processing Agreement shall be made available to the Customer free of charge upon request.

SECTION B: BASIC INFORMATION SECURITY REQUIREMENTS AND DATA PROTECTION

14. SECURITY GOVERNANCE

14.1 Compliance with standards and frameworks

14.1.1 The Supplier shall achieve and maintain information security and data protection compliance in accordance with;

a) ISO 27001:2022, NIST Cybersecurity Framework or other substantially equivalent standard(s) for information security management and any updates to such standards;

b) cloud specific frameworks, such as ISO 27017, CCM-CSA, C5 and FedRAMP.

14.2 Information security management system

14.2.1 The Supplier shall establish and maintain an effective information security management system that addresses all information security risks, including both external threats and

insider risks. The Services shall comply with requirements set forth in ISO 27001:2022 or equivalent standards.

14.2.2 Upon request by the Customer, the Supplier shall provide documentation that verifies independent assurance of the Supplier's information security management system through ISO 27001:2022 certifications, SOC2 Type 2 reports, C5, FedRAMP or equivalent evidence. The Supplier shall maintain the assurance at an equivalent or higher level throughout the duration of the Call-Off Contract.

14.3 Security audit and security testing obligations

14.3.1 The Supplier shall ensure the security of the Service(s) through regular external and internal security audits and security testing. Upon request by the Customer, the Supplier shall provide specifications of the type of testing performed, including which business processes are in scope for the testing requirements, e.g., change management and release management, and the frequency of such testing.

14.3.2 The Supplier shall address any issues identified in a security audit or security testing that are relevant to the Service(s) without undue delay and provide the Customer with the copy of the security audit or testing report upon request.

14.4 Access to security documents

14.4.1 The Supplier shall upon request make available to the Customer security policies and related security documents necessary to demonstrate compliance with the obligations laid down in the Call-Off Contract.

14.5 Third party security management

14.5.1 The Supplier shall ensure that third parties (e.g., vendors, services, subcontractors, and software providers) used in providing the Services to the Customer under the Call-Off Contract meet the security requirements set out in this Framework Agreement and the Call-Off Contract.

14.5.2 The Supplier shall notify the Customer in advance of any planned changes to the ownership or operation of the data centres or infrastructure used to deliver the Services. Such notice shall include the identity of the new third-party owner or operator, if applicable, and any potential impact on the provision of the Services.

15. COOPERATION REGARDING INFORMATION SECURITY

15.1 The Supplier shall appoint an information security responsible under the Call-Off Contract as a counterpart to the Customer, who is responsible for strategic security meetings, reporting, and management of material risks, incidents, and vulnerabilities. The Customer shall be entitled to escalate any issues to the responsible at executive level or DFØ.

15.2 Both Parties can summon a meeting with 7 (seven) days' written notice.

16. INCIDENT AND VULNERABILITY MANAGEMENT

16.1 Security incident management and threat intelligence

16.1.1 The Supplier shall establish and maintain processes for security incident management and threat intelligence. This includes to actively detect, identify and respond to threats and security incidents, including those arising from third parties or third-party components in the Service(s).

16.1.2 In the event of a serious security incident relating to the Services in general or affecting the Call-Off Contract, the Supplier shall immediately report in writing directly to the Customer, and no later than an initial warning within 24 hours and a report of the incident within 72 hours. The report shall include information about the systems, services and information affected, along with an assessment of the impact on the Customer and a remediation plan.

16.1.3 In the event of a serious security incident, the Supplier shall cooperate with relevant vendors of the Customer, such as ICT outsourcing partners, cloud vendors and managed security services providers appointed by the Customer, to ensure the operational information security of the Customer's systems.

16.1.4 The Supplier shall maintain and on request from the Customer provide access to a security log of all incidents concerning Customer Data, including log data and relevant indicators of compromise, for Customer incident analysis and digital forensic purposes.

16.1.5 The Supplier shall perform threat intelligence and continuously, or at least daily, update indicators of compromise (IoCs) and malware definitions.

16.1.6 The Supplier shall, while performing under the Call-Off Contract, ensure that all software and storage media used in the performance of the Service(s) is free of any malicious software.

16.2 Vulnerability management

16.2.1 The Supplier shall establish and maintain processes for managing vulnerabilities in the Services. This includes performing security patching and implementing other compensating measures according to defined service level agreements.

16.2.2 The Supplier shall monitor third-party vulnerability notifications and other relevant security vulnerability advisories.

16.2.3 Each vulnerability identified in the Service(s) shall be assigned a unique Common Vulnerability and Exposures ("**CVE**") identifier and a Common Vulnerability Scoring System ("**CVSS**") score. The Supplier shall maintain a record of all identified vulnerabilities.

16.2.4 The Supplier shall notify the Customer without undue delay of any vulnerabilities identified in the Services with a CVSS score of 9.0 to 10.0 (Critical) or 7.0 to 8.9 (High). The notification shall include information about the systems and information affected, along with an assessment of the impact on the Customer, and a remediation plan. The Supplier shall provide necessary support and information to the Customer and take appropriate actions to manage and mitigate risks associated with such vulnerabilities.

16.3 Suspension of service due to security incidents or vulnerability

16.3.1 In the event of a serious security incident or vulnerability in the Services, the Supplier shall offer to suspend the Services until the situation has been resolved or the Supplier has remedied the issue to the Customer's satisfaction. The Supplier shall assist the Customer with suspending the Services upon request.

16.4 Penetration testing rights

16.4.1 The Customer under the Call-Off Contract, shall, by itself or by use of a third party, have the right to perform penetration testing of the Services according to agreed routines, to identify and analyse any potential security vulnerabilities and risks.

17. ACCESS CONTROL AND CUSTOMER DATA

17.1 Security access management

17.1.1 The Supplier shall implement and maintain strict access control policies and procedures to ensure that only identified and authorised personnel have access to the Service(s) and their management system. The policies must, at minimum, address privileged access management, password management, authentication, authorisation, provisioning, and revocation of terminated users, separation of duties, approval workflows, and just-enough and just-in-time administration.

17.1.2 The Supplier shall conduct regular access review to ensure compliance with the established access control policies and procedures.

17.2 Flexible and fine-grained identity and access management

17.2.1 The Supplier shall provide the Customer with flexible and fine-grained mechanisms for identity and access management. This includes facilitating integration with the Customer's existing identity and access management systems, such as user directories.

17.2.2 The Supplier shall support relevant standards such as SCIM 2.0 or IETF RFC 7643 for cross-domain identity management.

17.3 Secure remote access

17.3.1 The Supplier shall ensure that any remote access to the Service(s) is secured with strong encryption and authentication measures in accordance with best industry practices, and that security gateways (enabling security policy enforcement, security monitoring, etc.) are used to control access between the Internet and the Supplier's Service(s).

17.4 Separation of Customer Data

17.4.1 The Supplier shall keep all Customer Data logically separate from the data of any third parties in order to eliminate the risk of compromising data and/or unauthorised access to data. Logically separate means the implementation and maintenance of necessary and technical measures to secure data against undesired change or access. Undesired changes or access shall include access by the Supplier's personnel or others who do not need access to the information in their work for Customer.

17.5 Encryption of Customer Data

17.5.1 The Supplier shall ensure protection of Customer Data in transit and at rest, both internally within the Service(s) and for inbound/outbound traffic, including web access, APIs and administrative accesses.

17.5.2 To achieve this protection, the Supplier shall implement measures such as state of the art encryption in transit, encryption at rest and strong authentication.

17.5.3 The Supplier shall support new available technologies regarding encryption and protection of Customer Data.

17.6 Logging of access to Customer Data

17.6.1 The Supplier shall maintain logs of all access to Customer Data by its own employees and any third parties and shall make such logs available to the Customer upon request.

17.6.2 The Parties shall agree on a retention period for the access logs under the Call-Off Contract, taking into account applicable Laws and regulations, as well as any recommendations from Norwegian national security and information security authorities.

17.7 Notification of relocation of Customer Data

17.7.1 The Supplier shall notify the Customer in writing in advance of any planned relocation or transfer of Customer Data, including backups, to a new data centre or any other location.

18. CHANGE MANAGEMENT AND SECURITY BY DESIGN

18.1 Change management

18.1.1 The Supplier shall establish and maintain strict procedures for technology change management and deviation handling in the Service(s).

18.1.2 The Supplier must provide advance notice to the Customer of any changes to the Service(s) that may negatively impact information security with sufficient time for the Customer to object.

18.2 Security by design

18.2.1 The Supplier shall implement and adhere to security by design principles in the provision of the Service(s) and ensure that software hardening best practices are implemented with secure configuration set as default.

18.2.2 The Supplier shall conduct testing to ensure that the Service(s) maintain a high level of integrity and quality, with no backdoors or known vulnerabilities.

18.2.3 The Supplier shall follow relevant industry standards and best practices to ensure security by design, such as CIS (https://www.cisecurity.org/), CWE/SANS Top 25 (http://cwe.mitre.org), OWASP Top 10 (http://www.owasp.org), and OWASP ASVS (https://owasp.org/www-project-application-security-verification-standard/).

19. BUSINESS CONTINUITY

19.1 Business continuity and disaster recovery

19.1.1 The Supplier shall establish and maintain business continuity and disaster recovery plans that adhere to best industry standards, such as ISO 22313. The plans shall include measures to prevent or mitigate the impact of various types of disasters or disruptions, including but not limited to ransomware attacks, a distributed denial-of-service attack ("**DDoS Attacks**"), advanced persistent threats ("**APT**") attacks, unavailability of external IT resources or other external authentication sources, sabotage, fire, and natural catastrophes. The Supplier shall regularly test and rehearse these plans to ensure their effectiveness in the event of a disaster or disruption.

19.1.2 The Supplier shall implement and maintain capacity management measures to ensure stable operations in both normal and disaster recovery situations.

19.2 Backup and restore of the Supplier's system

19.2.1 The Supplier shall conduct regular backups, including offline backups, and restore testing to ensure the integrity and availability of its systems.

20. PHYSICAL AND PERSONNEL SECURITY

20.1 Physical security

20.1.1 The Supplier shall implement and maintain appropriate physical security measures for its data centres, cloud infrastructure, operations environments (including remote operations), and any equipment installed on Customer premises, in accordance with relevant international standards and the Supplier's own policies.

20.1.2 The Supplier shall conduct annual audits of its physical security measures by an independent, qualified auditor certified to evaluate compliance with applicable standards and policies.

20.2 Personnel security

20.2.1 The Supplier shall ensure that all personnel involved in the delivery of the Service(s), including personnel of any Subcontractors and third parties, have committed themselves to confidentiality, receive appropriate training and maintain necessary expertise on security matters. This shall include training on applicable security rules, regulations and standards, including Customer-specific security rules where applicable.

20.2.2 The Supplier shall establish and maintain procedures for personnel security, including screening and background checks, to ensure that all personnel have the appropriate level of security clearance in accordance with best industry practice and any applicable Laws.

20.2.3 The Supplier is required to perform annual security audits on these procedures, conducted by a third-party auditor, to evaluate compliance with applicable standards and policies.

21. DATA PROTECTION

21.1 Introduction

21.1.1 The obligations and requirements set out in this clause 21 applies when the Supplier processes Personal Data under the Call-Off Contract and comes in addition to the Supplier's other obligations under the Call-Off Contract.

21.1.2 The Parties roles with regard to the processing, i.e., whether they act as data controller and/or data processor under the General Data protection Regulation (GDPR) (EU) 2016/679, is specified in Appendix 5.2.

21.2 Competence, training, and awareness

21.2.1 The Supplier shall ensure and document that authorised personnel, including any of its data processors or sub-processors, have the necessary competency and training within privacy and data protection in accordance with best industry practice, and applicable Laws.

21.2.2 The Supplier shall on regularly basis evaluate the competency and training of their personnel, including an assessment of the actions and measures implemented.

21.2.3 The Supplier shall build and maintain a culture to ensure that all relevant personnel receive appropriate awareness training to understand their responsibilities for data protection and information security.

21.3 Data processing agreement

21.3.1 If the Supplier processes Personal Data on behalf of the Customer as a data processor, the Customer and the Supplier are obliged to enter into a data processing agreement in accordance with the GDPR Art. 28 and any sector-specific data protection legislation that is relevant to the Customer's activities. A full and final data processing agreement shall be signed and binding by the Customer and the Supplier prior to processing of Personal Data.

21.3.2 As a default, the Supplier agrees to enter into the EU Standard Contractual Clauses (EU DPA) between controllers and processors under GDPR Art. 28. A template data processing agreement to be used by the Parties is attached to Attachment 4.2.1 (*Template EU DPA*). The Parties may, as an alternative, enter into the Supplier's standard data processing agreement if the Customer agrees. If the Parties enter into the Supplier's standard data processing agreement, the Supplier's data processing agreement shall be interpreted in accordance with Attachment 4.2.1, and in case of ambiguities or conflict between the EU DPA and the Supplier's standard processing agreement, the most favourable outcome for the Customer shall apply.

21.3.3 If the Customer has specific requirements as to how the Supplier shall process Personal Data, including additional technical and organisational measures, this shall be agreed in the Call-off Contract.

21.4 The Customer's instructions and the role of the Parties

21.4.1 If the Supplier processes Personal Data on behalf of the Customer, the Supplier shall process Personal Data only on documented instructions from the Customer, unless required to do so by EU/EEA or Member State law to which the Supplier is subject. The

Customer's instructions shall be specified in the Data Processing Agreement or Call-Off Contract.

21.4.2 The Supplier shall not process Personal Data for any other purposes (including its own purposes) other than those set out in the Call-Off Contract, the Data Processing Agreement or subsequent documented instructions from the Customer. The Supplier shall not process Personal Data to a greater extent than necessary to fulfil the aforementioned purposes. The Supplier may not determine what kind of processing they are authorised to do.

21.4.3 The Supplier shall only process and store Personal Data about the Customer's administrators and end-users, including the Customer's use of the Services, when and to the extent such processing is necessary to perform the Supplier's obligations under the Framework Agreement and the Call-Off Contract. The Supplier shall upon request from the Customer document how only required Personal Data about such users is registered, stored and processed.

21.5 Personal Data controls and measures

21.5.1 The Supplier shall implement and maintain an internal control system for the processing of Personal Data in accordance with applicable Law(s) and industry best practice, e.g. by adherence to approved codes of conduct or approved certification mechanisms as referred to in GDPR Arts. 40 and 42. The internal control system shall be reviewed and updated regularly.

21.5.2 The Supplier shall have a data protection officer when required according to GDPR Art. 37.

21.5.3 The Supplier shall upon request document the following:

a) how data protection is organised, managed and controlled in its business and supply chain, including clearly defined roles and responsibilities;

b) how Personal Data is processed in the Services, including the systems used, data flows and any processors or sub-processors processing, including what and why they process; and

c) the responsibilities and authorities for roles of privacy and data protection, including between the Customer, the Supplier and, where applicable, the Suppliers' sub-processors.

21.6 Collaboration regarding Personal Data

21.6.1 The Supplier shall collaborate with the Customer to ensure the protection and compliance of processing of Personal Data.

21.6.2 The Supplier shall notify the Customer immediately if it considers that any of the Customer's documented instructions infringe applicable data protection legislation.

21.6.3 The Supplier shall provide all reasonable assistance to the Customer to enable the Customer to comply with the data protection legislation. This includes, but is not limited to upon request:

a) provide the Customer with an assessment of the necessity and proportionality of the processing operations in relation to the Services;

b) assist the Customer with an assessment of the risks to the rights and freedoms of Data Subjects, including, but not limited to Transfer Impact Assessment (TIA) and/or Date Protection Impact Assessment (DPIA) where applicable; and

c) provide the Customer with information on measures envisaged to address the risks, including safeguards, security measures, and mechanisms to ensure the protection of Personal Data.

21.6.4 The Supplier shall notify the Customer without undue delay, and no later than 48 hours where:

a) the Supplier becomes aware of an incident resulting in loss of the Customer's Personal Data, or an incident that could have resulted in unauthorised access or disclosure of Personal Data;

b) receiving any communication from the Norwegian Data Protection Authority (in Norwegian: "Datatilsynet") or any other regulatory authority in connection with Personal Data processed under this Call-Off Contract.

21.6.5 The Supplier shall notify the Customer as soon as possible if it receives:

a) a request made by, or on behalf of, a Data Subject in accordance with rights granted pursuant to the Data Protection Legislation to access their Personal Data (Data Subject Request;

b) a request to rectify, block or erase any Personal Data;

c) a request from any third party for disclosure of Personal Data where compliance with such request is required or purported to be required by law; or

d) any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation.

21.7 Description of processing activities by Supplier and its data processors or sub-processors

21.7.1 The Supplier shall upon request provide or make available to the Customer a detailed description of the processing activities carried out by the Supplier and any of its data processors or sub-processors, and the purpose of the processing. This description shall include at a minimum:

a) the specific processing activities in which the Supplier and data processor or sub-processor will be involved, including which Service(s) that contain Customer Data the data processor or sub-processor will have access to;

b) the circumstances under which the data processor or sub-processor will have access to Personal Data, including whether access is continuous or only granted periodically or upon the Supplier's instructions; and

c) the categories of Personal Data that is processed by the Supplier and data processor or sub-processor and which processing activities the Personal Data is processed in.

21.8 Data protection by design and default

21.8.1 The Supplier shall provide the Services in accordance with data protection by design and by default principles throughout the lifecycle of the service, in accordance with GDPR Art. 25.

21.9 Data Subject's rights

21.9.1 The Supplier shall have solutions that enables the Customer to, in an efficient manner, fulfil the natural persons' rights according to GDPR, including rights to access, to be informed, to rectification, erasure, and data portability.

21.10 Locations and transfer of data

21.10.1 Personal Data shall not be transferred outside EU/EEA unless explicitly agreed with the Customer in the Call-Off Contract, the Data Processing Agreement, if relevant, and/or in accordance with the procedures set out in this clause.

21.10.2 Any transfer of Personal Data to countries outside the EU/EEA ("Third Country") shall be in accordance with GDPR chapter V Transfers of personal data to third countries or international organisation, prior to such transfer. Transfer includes, but is not limited to:

a) processing of Personal Data in data centres, etc. located in a Third Country, or by personnel located in a Third Country (by remote access)

b) assigning the processing of Personal Data to a data processor or sub-processor in a Third Country; or

c) disclosing Personal Data to a Data Controller in a Third Country, or to an international organisation.

21.11 Surveillance laws

21.11.1 The Supplier shall document and notify the Customer immediately if the Supplier, or its data processor or sub-processors, have been, are or become subject to any laws relating to the monitoring, observation, interception or surveillance of data that may undermine the obligations according to the GDPR.

21.12 Sub-processors

21.12.1 If the Supplier acts as data processor, the Supplier's general or specific authorisation to engage sub-processors shall be specified in the Data Processing Agreement. A general authorisation in the Data Processing Agreement only applies to sub-processors in the EEA. The Supplier shall not engage sub-processors outside the EEA without the Customer's prior specific authorisation unless otherwise is specifically and explicitly agreed in the Call-Off Contract.

21.12.2 The Supplier shall upon request document the controls, processes, and frameworks, including risk assessments used to assess, approve, evaluate and follow up sub-processors from a data protection perspective.

21.12.3 The Supplier shall upon request document data protection compliance of sub-processors.

21.13 New sub-processors

21.13.1 If the Supplier, when acting as data processor, has a general authorisation from the Customer for the engagement of sub-processors, the Supplier shall notify the Customer in writing of any new sub-processors minimum 45 days prior to the engagement of such sub-processor.

21.13.2 The Customer shall have the right to object to the engagement of new sub-processors in accordance with the Data Processing Agreement, SCC and GDPR Art. 28. If the Customer does not object within the 15 days, the sub-processor is deemed approved. If the Customer objects to the engagement of a new sub-processor, the following procedure shall be followed:

a) The Supplier shall provide a written explanation as to why the processing of Personal Data by the sub-processor is in accordance with applicable Laws, and how the use of the sub-processor will not compromise the information security under the Call Off-Contract. In addition, the Supplier shall address any objections raised by the Customer regarding the engagement of the sub-processor.

b) If the Customer still objects to the engagement of the new sub-processor, the Supplier shall use its best efforts to provide the Services without engaging the objected sub-processor, while ensuring that an equivalent level of information security is maintained.

c) The Customer may escalate the question regarding a new sub-processor to be resolved by DFØ.

d) If the Supplier cannot provide the Services without engaging the objected sub-processor, then Customer shall have the right to: (i) terminate the Call-Off Contract, or relevant Services under a Call-Off Contract, with immediate effect without any liability; or (ii) continue to use the Services but elect to be no longer bound by any Minimum Commitment applicable to the relevant Call-Off Contract. Upon termination the Supplier shall comply with the exit obligations set out in the Call-Off Contract without additional fees.

e) in either circumstance under d) above: (i) any related Minimum Commitment shall void and, in the event of the Customer having made any prepayment of Minimum Commitment, the Supplier shall refund an amount corresponding to the difference between prepaid Minimum Commitment and the Services actually accrued; and (ii) in addition the Supplier shall implement mitigating measures addressing the Customer's concerns, such as monitoring, reporting, and logging to maintain the same level of information security as before.

21.14 Transfer of requirements and obligations to the sub-processor

21.14.1 If the Supplier, when acting as data processor, engages a sub-processor for carrying out specific processing activities on behalf of the Customer, the same data protection obligations as set out in the Framework Agreement and the Call-Off Contract, including the completed Data Processing Agreement, shall be imposed on that sub-processor by way of a contract or other legal act under EU/EEA or Member State law, which shall provide sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the GDPR. Where that sub-processor fails to fulfil its data protection obligations, the Supplier shall remain fully liable to the Customer for the performance of that sub-processor's obligations.

21.15 Changes and guidance

21.15.1 The Parties agree to take account of any guidance issued by the Norwegian Data Protection Authority (in Norwegian: "Datatilsynet") and the European Data Protection Board (EDPB). The Customer may at any time with 30 days written notice to the Supplier:

a) revise the clauses relating to Data Protection to ensure that it complies with any guidance, codes of practice, codes of conduct, regulatory guidance, standard clauses or any other related laws arising from the GDPR.