Publication of Memorandum of Information II

Nr.	Subject	Question	Answer
31	Liability, Enexis Purchasing Conditions 2025	We have a follow-up question to question 27 in the Memorandum of information I. Since Enexis' answer to this question is crusial for the Candidate's decision to submit an offer or not, we urge Enexis to answer this as soon as possible and preferable before 18 May. Enexis is estimating that the Assignment will have a total estimated value of € 1 600 000 at a maxium. According to Enexis Purchasing Conditions 2025, this will limit the parties liability to € 3 000 000 per event and € 5 000 000 per contract year. As mentioned in question 27, this is not in line with market practice and put a disproportionally high level of risk on the Contactor. Can Enexis accept these suggested changes to art. 16.1? 16.1 The liability of the parties arising from a failure to perform the agreement attributable to them is limited to: • for agreements with a yearly total (estimated) value less than or equal to €50,000: €50 000 per event and €150 000 per contract year or part of a year during which the agreement is in force; • for agreements with a yearly total value exceeding €50,000 but less than or equal to €100,000: €100 000 per event and € 250 000 per contract year or part of a year during which the agreement is in force; • for agreements with a yearly total value exceeding €100,000 but less than or equal to €150,000: €150 000 per event and € 500 000 per contract year or part of a year during which the agreement is in force; • for agreements with a yearly total value exceeding €150,000 but less than or equal to €500,000: € 200 000 per event and € 1 000 000 per contract year or part of a year during which the agreement is in force; • for agreements with a yearly total value exceeding €500,000: € 500 000 per event and € 2 000 000 per contract year or part of a year during which the agreement is in force. Related events shall be regarded as a single event. If the failure relates to a Purchase Order/Assignment under a framework agreement, the total yearly value of the framework agreement shall be used as the basis for determining the total estimated value referred to in this clause. If Enexis cannot accept these suggested changes, can Enexis suggest an alternative model which places less liability on the parties?	Enexis will answer the questions as soon as possible. Enexis does not fully agree with your proposal. Enexis has amended Article 16.1 of the Enexis Purchasing Conditions 2025 in response to your question as follows (see Article 4.1 sub b of the Agreement): *The liability of the parties arising from a failure to perform the agreement attributable to them is limited to:* *•for agreements with a total (estimated) value less than or equal to €50,000: €50,000 per event and €150,000 per contract year or part of a year during which the agreement is in force;* *•for agreements with a total value exceeding €50,000 but less than or equal to €100,000: €100,000 per event and € 250,000 per contract year or part of a year during which the agreement is in force;* *•for agreements with a total value exceeding €100,000 but less than or equal to €150,000: €150,000 per event and € 500,000 per contract year or part of a year during which the agreement is in force;* *•for agreements with a total value exceeding €150,000 but less than or equal to €500,000: € 200,000 per event and € 1,000,000 per contract year or part of a year during which the agreement is in force;* *•for agreements with a total value exceeding €500,000: € 500,000 per event and € 2,000,000 per contract year or part of a year during which the agreement is in force.* *Related events shall be regarded as a single event.* *If the failure relates to a Purchase Order/Assignment under a framework agreement, the total yearly value of the framework agreement shall be used as the basis for determining the total estimated value referred to in this clause.*
32	Liability, Enexis Purchasing Conditions 2025	We have a follow-up question to question 27 in the Memorandum of information, which consisted of two questions; one question about limitation of liability and one question about indirect and consequential damages. Can Enexis agree that the Parties shall not under any circumstances be liable for indirect losses or consequential losses, including, but not limited to business interruption, loss of profit, loss of data, savings that have not materialised, losses of and claims from third parties or other financial consequential losses? If not, please elaborate why.	Enexis understands that Tenderers may have questions regarding liability provisions. Therefore, Enexis clarifies that Article 16.1 (Article 4.1 sub b of the Agreement) applies exclusively to damage attributable to the Contractor. For this tender, Enexis exclude liability for indirect damage. Indirect damage refers to lost profits, lost revenue or benefit, unrealized savings, production loss or downtime, or loss of goodwill or reputational damage. Enexis has added article 5.1 sub d to the Agreement. *Article 5.1 sub d: Enexis exclude liability for indirect damage. Indirect damage refers to lost profits, lost revenue or benefit, unrealized savings, production loss or downtime, or loss of goodwill or reputational damage.*
33	Payment	Could Enexis clarify the intended billing structure for the initial contract term of two years? Specifically, should Contractors assume that the costs for the Phishing Simulation and Phishing Incident Response solution will be invoiced upfront for the full two-year period, based on the actual number of End users at the start of the contract term?	The billing structure is such that invoicing will occur annually based on the actual number of End users.
34	Reliance on standard assurance reporting	Can Enexis confirm that commonly accepted third-party assurance materials such as ISO 27001 certifications, SOC 2 Type II reports, ISAE 3402 reports, penetration-test attestations and completed security questionnaires will be considered before requesting dedicated supplier audits?	Enexis reserves the right to request additional clarification, evidence or where necessary, a dedicated audit if the provided assurance materials do not sufficiently cover the relevant scope, controls, risks or services applicable to Enexis
35	Audit scope and proportionality	Can Enexis confirm that any audit rights applicable to SaaS suppliers will be limited to controls, evidence and documentation relevant to the Enexis services, and will not require unrestricted access to multi-tenant environments, source code or data relating to other customers?	Enexis does not require unrestricted access to multi-tenant environments, source code or data relating to other customers. Where direct access is not appropriate due to confidentiality, security or multi-tenant restrictions, Enexis may request alternative evidence such as third-party assurance reports, certifications, audit reports, control descriptions, screenshots, attestations or other relevant documentation.
36	Penetration-test reporting	Can Enexis confirm whether an executive summary, attestation letter or independent assurance statement from a third-party penetration test is sufficient where the full technical penetration-test report contains confidential information regarding the supplier's SaaS environment or other customers?	Enexis may request additional clarification or evidence if the provided summary or attestation does not sufficiently demonstrate that relevant findings have been addressed or that risks for Enexis are adequatly mitigated. Enexis will always treat the provided information as confidential.
37	Central role assignment	Can Enexis confirm that centrally managed role mapping through identity provider groups and claims into application roles is acceptable?	Yes. Enexis prefers the assignment of applicable functional application roles based on its own identity provider groups, for example via SCIMv2.
38	SSO-only access and emergency accounts	The requirements state that SSO must be the only way of logging in and that no accounts may be managed locally. Can Enexis clarify whether tightly controlled break-glass or emergency administrator accounts are acceptable for business continuity and incident recovery purposes?	This is acceptable, given that these are only used for these purposes and sufficient security controls and procedures are in place to prevent misuse.
39	Adaptive difficulty	Can Enexis clarify whether "adaptive difficulty level" may be achieved through configurable rules, targeting logic and performance-based campaign segmentation, rather than requiring a fully autonomous AI-driven learning model?	Both approaches are allowed.
40	Q5	Can Enexis confirm whether the Dutch and English language requirement applies only to the phishing simulation content and user-facing material proposed for Enexis, rather than to the supplier's complete global content library?	Enexis confirms this. All interfaces and training content **for Enexis** must be made fully available to End users in both English and Dutch and all content must be provided both in Dutch and English. All video and audio material **for Enexis** must be available in both languages. Only using subtitles isn't allowed. The global content library is not part of this requirement. We don't have requirements for content that won't be proposed to Enexis.
41	Q17	MoI I clarifies that computer-based training and e-learning modules are out of scope, while phishing simulations and related reporting are in scope. Can Enexis confirm that references to "security training" should therefore be interpreted as simulation-based learning and feedback rather than a requirement for a full e-learning library?	Our references to "security training" mean to reflect Continuous phishing, without specifying the form of learning itself. Other computer security subjects are considered out-of-scope.
42	Integration scope	Requirement PIR2.2.1 refers to integration with Microsoft Defender/Sentinel or ServiceNow Security Incident Response. Can Enexis confirm whether integration with one supported workflow route is sufficient, or whether integrations with all listed platforms are expected?	Integration with only one of the applications is sufficient and expected.
43	Q21	Can Enexis confirm that the Contractor may provide implementation guidance, integration documentation and technical support without requiring direct administrative access to Enexis' Microsoft Defender, Sentinel or ServiceNow environments?	Enexis prefers that administrative activities in Enexis controlled environments are performed by Enexis or by parties explicitly authorized by Enexis. If direct access by the Contractor is exceptionally required, this must be agreed in advanced and must comply with Enexis access management, security and logging requirements.
44	Q21	Can Enexis confirm that the Contractor may provide implementation guidance, integration documentation and technical support without requiring direct administrative access to Enexis' Microsoft Defender, Sentinel or ServiceNow environments?	See the answer to question 43.
45	Q22	MoI I indicates that Enexis SOC remains responsible for substantive handling and mitigation decisions. Can Enexis confirm whether the proposed solution is expected to support and initiate purge workflows, while final approval and execution of tenant-wide delete actions may remain with Enexis SOC?	If the Tenderer offers, based on a weighted or proven level of assurance, the possibility to perform fully automated mitigating actions within agreed boundaries, Enexis will certainly consider using that functionality. In the Proposal, we would therefore welcome an explanation of the considerations the Tenderer makes when offering such functionality and which conditions and limitations they recommend. Where full automation in that regard would not be possible or permissible, the Enexis IT SOC remains fundamentally responsible for that activity.
46	Tenant-wide search and delete	Can Enexis clarify whether "tenant-wide search and delete" must be executed directly by the proposed PIR solution itself, or whether orchestration through Microsoft Defender, Microsoft Graph, Microsoft Purview, Sentinel or another Enexis-controlled platform is also acceptable?	It is acceptable to make use of existing functionality of the mentioned products.
47	AI model training	Can Enexis confirm that Enexis data, personal data, email content and incident data may not be used to train, fine-tune or improve general-purpose AI models or shared services outside the dedicated Enexis environment unless explicitly agreed in writing?	Enexis confirms this.
48	AI assisted functionality	Can Enexis clarify whether AI-assisted capabilities such as phishing classification, summarization, template generation, risk scoring or threat analysis are permitted, provided that Enexis data remains within the agreed privacy and data residency boundaries?	The agreed privacy, confidentiality and data residency requirements applicable to this Assignment remain fully applicable to any AI-supported functionality. In particular, Enexis expects that: •Enexis data remains within the agreed EU/EEA hosting, processing and management boundaries; •AI-related processing activities are transparent and appropriately documented; •no Enexis data is used for training, retraining or improving shared or public AI/ML models unless explicitly agreed in writing; •suppliers provide transparency regarding any third-party AI providers, subprocessors or external model providers involved; and •appropriate technical and organisational safeguards are implemented to protect the confidentiality, integrity and availability of Enexis data. In addition, Enexis expects that proposed AI-assisted functionalities do not qualify as prohibited, high-risk or otherwise materially regulated AI use cases under applicable AI legislation, including the EU AI Act, unless explicitly disclosed and agreed in advance. Where AI capabilities rely on external platforms, APIs, subprocessors or processing environments outside the agreed contractual and jurisdictional boundaries, this must be explicitly disclosed and will be subject to separate assessment and prior written approval by Enexis. Enexis reserves the right to assess proposed AI functionalities on a case-by-case basis, taking into account privacy, information security, regulatory compliance, explainability and operational risk considerations.
49	DPA	The DPA states that processing or transfer outside the EEA is not permitted, while also describing a mechanism for international transfers subject to prior consent, SCCs and a DTIA. Can Enexis confirm whether international transfers are entirely prohibited for this Assignment, or whether Enexis may permit limited transfers under the conditions described in the DPA?	Enexis' starting point for this Assignment is that the processing, storage and management of personal data must take place entirely within the EEA. This follows from the nature of the services, the applicable information security requirements, and Enexis' internal compliance and risk management frameworks. The provisions in the DPA regarding international transfers are included to provide a legal framework for situations in which a limited transfer outside the EEA is demonstrably necessary. However, this does not mean that such transfers are permitted by default. Any proposed transfer outside the EEA will only be considered subject to Enexis' prior written approval and under strict conditions. In this context, the Supplier must at minimum: •provide full transparency regarding all relevant entities, locations, subprocessors and support structures; •demonstrate why the transfer is necessary for the performance of the services; •implement appropriate safeguards, including applicable SCCs; •provide an up-to-date DTIA/TIA demonstrating that an adequate level of protection is ensured; and •implement additional technical and organisational measures where relevant, such as encryption, access restrictions and data minimisation. Enexis reserves the right to reject any proposed international transfer where the associated risks relating to privacy, information security, business continuity or regulatory compliance are considered insufficiently mitigated.

50	managed exclusively within the EEA	Can Enexis clarify whether "managed exclusively within the EEA" includes operational administration, security monitoring, incident response support, backup management and privileged administrative access to the SaaS environment?	For Enexis, the requirement that the SaaS environment is "managed exclusively within the EEA" is not limited to the physical hosting location of the data. The requirement also extends to operational and administrative activities that may involve access to, visibility of, or influence over personal data or the production environment. This includes, but is not limited to: •operational administration and platform management; •security monitoring and security operations activities; •incident response and support activities; •backup and recovery management; •privileged administrative access; •remote support activities; and •maintenance activities performed on production systems containing Enexis data. Enexis expects these activities to be performed from within the EEA and by entities/personnel operating under EEA jurisdiction. This requirement is intended to limit exposure to non-EEA legislation, governmental access risks and international transfer risks. Where a supplier believes that certain limited support activities from outside the EEA are technically unavoidable, this must be explicitly disclosed and substantiated by the supplier. Any exception will be subject to prior written approval by Enexis and requires: •a clear description of the activity and scope of access; •implementation of strict access controls and logging; •demonstration of necessity and proportionality; •appropriate transfer safeguards, including SCCs where applicable; and •a completed DTIA/TIA together with any additional technical and organisational safeguards required by Enexis. Enexis reserves the right to assess such requests on a case-by-case basis and to reject proposed arrangements that do not sufficiently mitigate privacy, security or compliance risks.
51	Processing and support	Enexis has clarified that all data must be stored, processed and managed exclusively within the EEA. Can Enexis confirm whether remote technical support or troubleshooting activities performed by personnel located outside the EEA are also prohibited if such personnel may have incidental access to Enexis data, metadata, logs or email content?	Enexis' position is that remote technical support or troubleshooting activities performed from outside the EEA are in principle not permitted where such activities may result in access to, visibility of, or exposure to Enexis data. This includes not only direct access to personal data, but also incidental access to metadata, system logs, telemetry, configuration data, audit trails, or email content processed within the SaaS environment. From Enexis' perspective, the location from which support activities are performed is relevant where personnel outside the EEA could reasonably obtain access to information relating to Enexis systems, users or communications, regardless of whether such access is structural, temporary, incidental or limited in scope. Suppliers are therefore expected to organise support, administration and incident response activities in such a manner that access to Enexis environments and related data remains within the EEA. Where a supplier believes that highly exceptional support activities from outside the EEA are technically unavoidable, this must be explicitly disclosed in advance and will only be considered subject to prior written approval by Enexis. In such cases, the supplier must clearly demonstrate: •why EEA-based support is not reasonably feasible; •the exact nature, duration and scope of the access; •which categories of data may become accessible; •which technical and organisational safeguards are implemented to minimise exposure; •how access is controlled, monitored and logged; and •which transfer mechanisms and DTIA/TIA measures are in place. Enexis reserves the right to reject any proposed support arrangement that, in its assessment, creates unacceptable privacy, security or compliance risks.
52	Nvl Q7	Would the contracting authority be willing to clarify whether the requirement regarding data processing exclusively within the EU/EER should be interpreted as an absolute restriction, or whether solutions that are fully GDPR-compliant but may involve limited supporting processing activities outside the EU/EER can also be considered acceptable?	The contracting authority's preference and primary requirement for this Assignment is that data processing, storage, management and operational support activities take place entirely within the EU/EEA. This requirement reflects not only GDPR compliance considerations, but also broader information security, confidentiality, supply chain and geopolitical risk considerations. The contracting authority recognises that certain SaaS solutions may involve limited supporting activities outside the EU/EEA, even where the solution is generally designed to operate in a GDPR-compliant manner. However, GDPR compliance alone is not considered sufficient automatically to satisfy the requirements applicable to this Assignment. Any processing or support activities outside the EU/EEA must therefore be regarded as exceptional rather than standard. Suppliers are expected to minimise such activities to the greatest extent possible and to provide full transparency regarding: •the nature and purpose of the activities; •the countries involved; •the entities and personnel involved; •the categories of data potentially affected; •the level of access involved; and •the safeguards implemented to mitigate transfer and access risks. Where limited non-EU/EEA supporting activities are proposed, the contracting authority may assess such arrangements on a case-by-case basis. Any potential acceptance remains subject to prior written approval and requires, at minimum: •implementation of appropriate transfer safeguards, including SCCs where applicable; •a completed DTIA/TIA demonstrating an essentially equivalent level of protection; •strict technical and organisational access controls; •logging and auditability of access; •data minimisation principles; and •a clear demonstration that the activities are necessary and proportionate. The contracting authority expressly reserves the right to determine that certain proposed non-EU/EEA processing or support arrangements are incompatible with the risk profile and security requirements of the Assignment, even where the supplier considers such arrangements to be GDPR-compliant.
53	Nvl Q7	We fully understand the underlying concerns regarding data sovereignty, privacy, and control. At the same time, the GDPR does not necessarily require that all processing always takes place exclusively within the EU/EER. The key requirement is that any international processing or transfer is transparent, contractually governed, and protected through appropriate legal, technical, and organizational safeguards, such as Data Processing Agreements (DPAs), Standard Contractual Clauses (SCCs), subprocessor transparency, and appropriate security measures. In practice, many widely adopted enterprise SaaS platforms used by European organizations may involve limited supporting activities outside the EU/EER, for example related to support services, monitoring, logging, notifications, or operational continuity, while still remaining fully GDPR-compliant. Could the contracting authority therefore confirm whether solutions with such limited and properly safeguarded international processing activities would remain eligible for consideration?	Enexis acknowledges that the GDPR does not impose a general prohibition on international data transfers and that, under the GDPR framework, transfers outside the EU/EEA may in principle be permissible where appropriate safeguards are implemented. The contracting authority also recognises that many enterprise SaaS solutions currently available on the market may involve certain limited supporting activities outside the EU/EEA. However, for this Assignment, the assessment is not limited solely to formal GDPR compliance. In addition to privacy legislation, the contracting authority must also consider information security, confidentiality, operational resilience, supply chain security, data sovereignty and exposure to foreign jurisdictional access risks. These considerations are particularly relevant in the context of critical infrastructure and security-sensitive environments. For that reason, the contracting authority's preference and default position is that processing, storage, administration and support activities relating to Enexis data remain fully within the EU/EEA wherever reasonably possible. Solutions involving limited international supporting activities may nevertheless be considered, provided that: •such activities are strictly limited in scope and demonstrably necessary; •the supplier provides full transparency regarding the nature of the activities, involved jurisdictions, subprocessors and access scenarios; •no structurally unrestricted or persistent access to Enexis data is involved; •appropriate legal safeguards are implemented, including SCCs where applicable; •a DTIA/TIA demonstrates that the level of protection is essentially equivalent to EU standards; •sufficient technical and organisational safeguards are implemented, including strong access controls, encryption, logging and data minimisation; and •the overall residual risk is considered acceptable by the contracting authority. The contracting authority expressly reserves the right to determine, at its own discretion, whether a proposed international processing arrangement is compatible with the risk profile and security requirements of the Assignment. Consequently, the existence of GDPR transfer mechanisms alone does not automatically render a solution acceptable.
54	Appendix 02 - Schedule of Requirements	We refer to requirements (1.1.4, CP1.2.2, PIR 2.3.4, 3.1.1, and CP4.2.4 – 4.2.8), where it is stated that "The Contractor" adhere to requirements. In other requirements, it is referred to the tooling must adhere to requirements. For consistency, could Enexis clarify if these formulations are correct, or if it in all requirements should be referred to the tooling?	The requirements you refer to are functional requirements. 1.1.4: This is a general requirement that applies to the Contractor. CP 1.2.2: This requirement relates to the Continuous phishing tooling. PIR 2.3.4: This requirement relates to the Phishing incident response tooling. 3.1.1: This is a requirement that applies to the Contractor. CP 4.2.4. - 4.2.8 are requirements related to the Continuous phishing tooling.