

25 SEPTEMBER 2026

**Marktconsultatieverslag Awareness/-e-learning
platform Informatiebeveiliging en Privacy**

Inleiding

1.1 Aanleiding marktconsultatie

De Veiligheidsregio Kennemerland (VRK) maakte gebruik van een e-learningplatform voor bewustwording op het gebied van informatiebeveiliging en privacy. Via dit platform werden periodiek verplichte trainingen aangeboden aan circa 1.400 medewerkers en vrijwilligers binnen de verschillende organisatieonderdelen van de VRK.

Awareness op het gebied van informatiebeveiliging en privacy vormt een belangrijk onderdeel van het informatiebeveiligingsbeleid van de VRK. Het draagt bij aan de naleving van relevante wet- en regelgeving en normenkaders, waaronder de AVG, BIO, AI Act, ISO 27001 en NEN 7510. Daarnaast wordt vanuit de cyberbeveiligingswetgeving steeds meer nadruk gelegd op aantoonbare bewustwording en training van medewerkers.

De VRK wilde inzicht verkrijgen in de mogelijkheden die de markt biedt om het awarenessprogramma verder te professionaliseren en toekomstbestendig in te richten. Daarbij bestond onder meer interesse in rapportages, managementinformatie, phishingsimulaties, microlearning, gamification, doelgroepgerichte content en andere vormen van gedragsbeïnvloeding en bewustwording.

Om inzicht te verkrijgen in beschikbare marktoplossingen, innovatieve ontwikkelingen, contractvormen, prijsmodellen en implementatiemogelijkheden heeft de VRK voorafgaand aan een mogelijke aanbesteding een marktconsultatie uitgevoerd. De resultaten worden betrokken bij het bepalen van de aanbestedingsstrategie, het vaststellen van de scope en het opstellen van een passend Programma van Eisen.

1.2 Doel van dit document

Dit document heeft als doel om de bevindingen vanuit de marktconsultatie, in het kader van een transparante procesvoering, in de vorm van een geanonimiseerd, algemeen samengevat verslag met partijen die een reactie hebben ingediend te delen. Dit document is uitdrukkelijk **niet** bedoeld als uitnodiging voor het doen van aanbiedingen.

1.3 Procedure marktconsultatie

Vragenronde

De VRK heeft een openbare marktconsultatie uitgevoerd ter voorbereiding op een mogelijke verwerving van een awareness-/e-learningplatform voor informatiebeveiliging en privacy. De markt is bevraagd over functionaliteit, content, rapportage, implementatie, beheer, prijsmodellen, contractvormen en aanbestedingsgerichte aandachtspunten.

Schriftelijke vragen

De VRK heeft via TenderNed 36 schriftelijke vragen aan de markt gesteld. Uiterlijk op 25 september 2026 hebben tien marktpartijen een inhoudelijke reactie ingediend. Eén partij heeft daarnaast een aanvullende productbeschrijving aangeleverd.

2 Vragen en antwoorden

De VRK heeft in de marktconsultatie onderstaande vragen gesteld. In dit verslag zijn de antwoord(richting)en van de partijen – naar beste inzicht van VRK – in algemene vorm samengevat en geanonimiseerd weergegeven. De antwoorden(richtingen) zijn op basis van de ingediende schriftelijke reacties.

Nr.	Vraag	Geanonimiseerde samenvatting van de markt
1	Kunt u uw organisatie kort voorstellen en aangeven wat uw kernactiviteiten zijn op het gebied van awareness, informatiebeveiliging en privacy?	De markt bestaat uit gespecialiseerde Nederlandse awarenessaanbieders, IT- en securitydienstverleners en bredere leerplatformleveranciers. Het aanbod varieert van integrale SaaS-platformen met eigen content tot platformen die content of phishing simulaties via partners leveren. De kern ligt steeds bij bewustwording, gedragsverandering, microlearning, phishingoefeningen, rapportage en begeleiding.
2	Welke organisaties in de (semi-)publieke sector, zorgsector of veiligheidssector maken momenteel gebruik van uw oplossing?	Meerdere partijen hebben ervaring bij gemeenten, veiligheidsregio's, zorgorganisaties, onderwijs, ministeries en andere (semi-)publieke instellingen. De mate van sector specifieke ervaring verschilt. Enkele aanbieders hebben nog geen referenties in zorg of veiligheidssector, maar wijzen op ervaring met vergelijkbare doelgroepen zonder vaste werkplek of organisatie emailadres.
3	Welke ontwikkelingen ziet u de komende drie jaar binnen de markt en wat is uw visie daarop?	De markt verwacht een verschuiving van jaarlijkse compliance-training naar continu en meetbaar veilig gedrag. Genoemd worden korte frequente interventies, adaptieve en doelgroepgerichte leerpaden, AI-gegenereerde dreigingen, vishing/smishing/quishing, realtime ondersteuning en auditklare bestuursrapportage. Tegelijk waarschuwen partijen voor awarenessmoeheid en een te grote leerbelasting.
4	Welke onderscheidende kenmerken heeft uw oplossing ten opzichte van vergelijkbare aanbieders?	Onderscheid wordt gezocht in didactische visie, storytelling, gamification, gedragswetenschappelijke onderbouwing, realistische simulaties, sector specifieke content, mobiele toegankelijkheid, personalisatie, automatisering, realtime coaching en integratie met de securitystack. De markt laat zien dat gamification verschillend wordt ingevuld; sommige partijen kiezen bewust voor scoreborden, andere juist niet.
5	Welke functionaliteiten biedt uw platform standaard voor e-learning op het gebied van informatiebeveiliging en privacy?	Vrijwel alle oplossingen bieden e-learning of microlearning, gebruikers- en groepsbeheer, automatische uitnodigingen en herinneringen, voortgangsregistratie, dashboards, doelgroepgerichte toewijzing en toegang via browser of mobiel. De omvang en aard van de contentbibliotheek verschillen sterk.
6	Welke aanvullende functionaliteiten zijn beschikbaar?	Veelgenoemd zijn phishing- en spearphishingcampagnes, nulmetingen, gamification, adaptieve leerpaden, doelgroepgerichte content, awarenesscampagnes, meldknoppen, managementdashboards en rapportages. Aanvullend worden onder meer realtime phishingassistenten, incidentdashboards, certificering, fysieke games, helpdesk-/triagediensten en koppelingen met BI- of securitysystemen aangeboden.
7	Welke functionaliteiten worden vaak onderschat, maar leveren in de praktijk veel toegevoegde waarde?	Als onderschat worden genoemd: meldgedrag en opvolging van meldingen, het teachable moment direct na een fout, automatische nudges, onboarding, teammanagers met beperkte rapportage toegang,

Nr.	Vraag	Geanonimiseerde samenvatting van de markt
		mobiele bereikbaarheid, herkenbare organisatiecontent, herhaalmetingen en de kwaliteit van interne communicatie.
8	Welke nieuwe functionaliteiten zijn momenteel in ontwikkeling?	De roadmaps richten zich vooral op AI-ondersteunde contentcreatie en simulaties, adaptievere leerpaden, vishing en smishing, verbeterde dashboards en actiegerichte rapportage, API- en Power BI-koppelingen, toegankelijkheid en realtime ondersteuning bij verdachte berichten. Niet alle aangekondigde functionaliteiten zijn al beschikbaar; dit moet bij aanbesteding aantoonbaar worden geverifieerd.
9	Hoe wordt de inhoud van trainingen actueel gehouden ten aanzien van wetgeving en actuele cyberdreigingen?	Partijen onderhouden content doorlopend of periodiek op basis van AVG, BIO, NIS2/Cyberbeveiligingswet, AI Act, NCSC-signalen en actuele aanvalsvormen. De actualisatiefrequentie varieert van doorlopend of binnen enkele weken tot halfjaarlijkse of jaarlijkse integrale herziening. Afspraken over urgente updates, inhoudelijke toetsing en meerkosten moeten contractueel worden vastgelegd.
10	In welke mate kan content worden aangepast aan de huisstijl, processen en risico's van de VRK?	De meeste oplossingen ondersteunen aanpassing van logo, kleuren, afzender, terminologie, beleid, meldroutes, scenario's en doelgroepindeling. De diepgang loopt uiteen van beperkte replacement-teksten tot volledig maatwerk, eigen content en opnames op locatie. Maatwerk kan een belangrijke prijs- en beheerfactor zijn.
11	Is content beschikbaar voor verschillende doelgroepen?	Ja. De markt kan differentiëren naar kantoorfuncties, operationele medewerkers, vrijwilligers, leidinggevenden en bestuurders. Veel partijen adviseren daarnaast differentiatie naar kennisniveau, risicoprofiel en toegang tot digitale middelen. Voor vrijwilligers en operationele medewerkers worden korte, mobiele en laagdrempelige leervormen aanbevolen.
12	Wordt de content zelfstandig ontwikkeld of door derden geleverd?	Een deel van de aanbieders ontwikkelt alle content in eigen beheer. Andere partijen combineren een eigen platform en maatwerkexpertise met content of simulaties van partners. De gekozen keten, verantwoordelijkheden, actualisatie, intellectuele eigendom en afhankelijkheid van onderleveranciers moeten transparant zijn.
13	Welke standaardrapportages zijn beschikbaar?	Standaardrapportages betreffen doorgaans deelname, afronding, kennis- en toetsresultaten, phishingresultaten, meldgedrag, risicoscores, trends en compliance/auditinformatie. Diverse oplossingen ondersteunen automatische periodieke verzending en export naar PDF, CSV of Excel.
14	Op welke niveaus kan worden gerapporteerd?	Rapportage is doorgaans mogelijk op organisatie-, onderdeel-, afdeling-, team-, doelgroep- en individueel niveau, afhankelijk van inrichting en autorisaties. Meerdere partijen adviseren individuele phishingsresultaten niet zonder meer aan leidinggevenden beschikbaar te stellen en privacy, proportionaliteit, OR en FG vooraf te betrekken.
15	Welke KPI's worden gebruikt om awareness en gedragsverandering inzichtelijk te maken?	Veelgenoemde KPI's zijn deelname, afronding, kennisscore, klik- en invoerratio, meldratio, tijd tot eerste melding, herhaalgedrag, actieve gebruikers en ontwikkeling ten opzichte van een nulmeting. De markt adviseert niet alleen op klikratio te sturen, maar vooral naar meldgedrag, trend en aantoonbare gedragsontwikkeling te kijken.
16	In hoeverre kunnen rapportages worden aangepast aan de behoeften van de opdrachtgever?	Dashboards en rapportages zijn meestal filterbaar en periodiek te distribueren. Maatwerkrapportages, bestuursrapportages, API's en BI-koppelingen zijn vaak mogelijk, maar niet altijd standaard inbegrepen of al productierijp. VRK moet vooraf informatiebehoefte, autorisaties, exportformaten en frequentie concretiseren.

Nr.	Vraag	Geanonimiseerde samenvatting van de markt
17	Wat is een gebruikelijke implementatieaanpak voor circa 1.400 medewerkers en vrijwilligers?	De gebruikelijke aanpak bestaat uit intake/design, technische inrichting, doelgroep- en contentafstemming, pilot of testgroep, nulmeting, gefaseerde uitrol en structurele evaluatie. Genoemde doorlooptijden variëren globaal van enkele weken tot circa tien weken, afhankelijk van koppelingen, contentmaatwerk, besluitvorming en gereedheid van gebruikersdata.
18	Welke inspanning wordt verwacht van de opdrachtgever tijdens implementatie en beheer?	VRK moet in ieder geval een inhoudelijk eigenaar/coördinator, technische contactpersoon en capaciteit vanuit informatiebeveiliging/privacy en communicatie beschikbaar stellen. Ook zijn besluiten nodig over doelgroepen, KPI's, content, scenario's, rapportagerechten en interne communicatie. De structurele beheerlast verschilt sterk per oplossing en mate van automatisering.
19	Welke koppelingen zijn beschikbaar met Microsoft Entra ID/Azure AD en Microsoft 365?	SSO met Microsoft Entra ID is breed beschikbaar. Veel partijen bieden geautomatiseerde provisioning/synchronisatie via SCIM, Microsoft Graph of een functioneel gelijkwaardige koppeling. Andere genoemde integraties zijn Outlook-meldknoppen, Teams-notificaties, Exchange/Defender, Power BI, HR-systemen en API's. De exacte rechten, attributen en technische verantwoordelijkheid moeten vooraf worden gespecificeerd.
20	Welke beheertaken blijven bij de opdrachtgever en welke verzorgt de leverancier?	De leverancier verzorgt doorgaans hosting, beveiliging, technisch beheer, updates, contentactualisatie en tweedelijns ondersteuning. VRK blijft veelal verantwoordelijk voor eigenaarschap, doelgroepbesluiten, interne communicatie, lokale content, opvolging van resultaten en incidenten en autorisatiebeleid. Een RACI/verantwoordelijkhedenmatrix wordt aanbevolen.
21	Welke rollen en autorisaties kent de oplossing?	Gebruikelijke rollen zijn gebruiker/deelnemer, team- of afdelingsmanager, content- of campagnebeheerder, organisatiebeheerder en soms auditor of superadmin. De markt biedt rolgebaseerde afscherming, maar de granulariteit verschilt. Privacy-by-design en minimale toegang tot individuele resultaten zijn belangrijke uitgangspunten.
22	Welke prijsmodellen worden gehanteerd?	De markt hanteert licenties per geregistreerde of actieve gebruiker, jaarlijkse abonnementen met staffels, vaste organisatiebrede tarieven en in enkele gevallen pay-as-you-go of projectmatige modellen. Contractduur, gebruikersvolume en scope beïnvloeden meestal het tarief.
23	Welke onderdelen zijn standaard inbegrepen en welke worden aanvullend gefactureerd?	Standaard zijn veelal platform, basiscontent, updates, dashboards, support en koppelingen inbegrepen. Phishing, maatwerkcontent, implementatie, workshops, uitgebreide begeleiding, realtime assistenten, aanvullende securitylagen, bijzondere koppelingen en managed services kunnen apart worden geprijsd. De markt hanteert geen uniforme scope.
24	Welke factoren en functionaliteiten hebben de meeste invloed op de totale prijsstelling?	Belangrijkste prijsfactoren zijn aantal en type gebruikers, contractduur, frequentie en complexiteit van phishing, hoeveelheid maatwerkcontent, implementatiebegeleiding, supportniveau, koppelingen en aanvullende diensten. De verhouding tussen beroepsmedewerkers en vrijwilligers kan materieel doorwerken in de prijs.
25	Wat is de indicatieve prijsbandbreedte voor circa 1.400 medewerkers en vrijwilligers?	De ontvangen indicaties lopen sterk uiteen door verschillen in scope en prijsmodel. Indicatieve jaarlijkse bedragen voor circa 1.400 gebruikers liggen grofweg tussen circa € 12.000 en € 50.000 exclusief btw, waarbij implementatie en optionele diensten niet altijd zijn inbegrepen. Enkele reacties zijn commercieel vertrouwelijk; daarom worden geen herleidbare leveranciersprijzen gepubliceerd.
26	Wat is de indicatie van de totale kosten over vier jaar?	Voor vier jaar lopen de vergelijkbare indicaties globaal uiteen van circa € 50.000 tot ruim € 200.000 exclusief btw. Bij uitgebreide

Nr.	Vraag	Geanonimiseerde samenvatting van de markt
		maatwerk- en aanvullende dienstverlening kan dit hoger uitvallen. Een betrouwbare raming vereist een vaste basisscope, uniforme prijsbijlage en afzonderlijke prijzen voor opties, implementatie, indexatie en exit.
27	Welke contractduur wordt doorgaans gekozen en welk effect heeft dit op de prijsstelling?	Veelgenoemd zijn looptijden van drie of vier jaar, dan wel twee jaar met verlengingsopties. Een langere looptijd kan het jaartarief verlagen en biedt ruimte om gedragsontwikkeling over meerdere meetmomenten te volgen. VRK moet flexibiliteit, evaluatiemomenten en doorontwikkeling afwegen tegen leveranciersafhankelijkheid.
28	Welke exit-mogelijkheden bestaan er bij beëindiging van het contract?	Partijen bieden doorgaans export van rapportages en gegevens, verwijdering van persoonsgegevens en soms migratieondersteuning. Formaten, termijnen, kosten, gebruiksrechten op maatwerkcontent en verwijdering uit back-ups verschillen. Dataportabiliteit, exitbijstand en een verwijderverklaring moeten vooraf contractueel worden vastgelegd.
29	Welke succesfactoren ziet u bij organisaties die veel rendement halen uit awarenessprogramma's?	Breed gedragen succesfactoren zijn zichtbaar eigenaarschap van directie en lijnmanagement, korte en frequente interventies, relevante doelgroepcontent, positieve no-blamecultuur, goede communicatie, nul- en herhaalmetingen, opvolging van meldingen en een vaste programmaverantwoordelijke.
30	Tegen welke implementatieproblemen lopen organisaties in de praktijk vaak aan?	Veelvoorkomende knelpunten zijn onvolledige Entra- of gebruikersdata, onduidelijkheid over vrijwilligersaccounts, gebrekkige mailaflevering/whitelisting, te late afstemming met OR/FG, onvoldoende communicatie, te hoge leerbelasting, generieke content en ontbrekend eigenaarschap na livegang.
31	Welke lessons learned geeft u de VRK mee bij selectie en implementatie?	De markt adviseert vooraf gedrags- en leerdoelen vast te leggen, een representatieve pilot en nulmeting uit te voeren, doelgroepen te differentiëren, vrijwilligers expliciet mee te nemen, beheerlast te testen, KPI's en privacykaders vooraf te bepalen en voldoende capaciteit voor communicatie en borging te reserveren.
32	Welke eisen worden vaak onnodig zwaar of beperkend geformuleerd?	Als onnodig beperkend worden genoemd: identieke sectorreferenties, disproportionele omzet- of certificeringseisen, voorgeschreven technische standaarden of leervormen, 24/7-support, eisen aan aantallen modules/talen, onbeperkt maatwerk, een exacte featurematrix en de eis dat één leverancier alles zelf uitvoert. Eisen moeten functioneel, proportioneel en resultaatgericht worden geformuleerd.
33	Welke eisen of wensen adviseert u juist wel op te nemen in het Programma van Eisen?	Veelgenoemde eisen/wensen zijn veilige EU/EER-dataverwerking, verwerkersovereenkomst, aantoonbare informatiebeveiliging, Nederlandstalige actuele content, digitale toegankelijkheid, SSO en automatische provisioning, doelgroepdifferentiatie, mobiele toegang, nul- en herhaalmetingen, privacyvriendelijke rapportage, meldgedrag als KPI, vaste evaluatiecyclus, beheerautomatisering en duidelijke exit/dataportabiliteit. Transparantie over AI-gebruik verdient een afzonderlijke eis.
34	Welke gunningscriteria maken volgens u het beste onderscheid tussen aanbieders?	De markt adviseert kwaliteitscriteria rond een live demo of praktijkscenario, didactische visie, herkenbaarheid van content, aanpak voor vrijwilligers en operationele medewerkers, implementatie en adoptie, rapportage, gedragsmeting, beheerlast, actualisatie en partnerschap. Een gebruikerspanel met een dwarsdoorsnede van de organisatie kan het onderscheid beter zichtbaar maken dan alleen schriftelijke plannen.
35	Welke onderdelen van de voorgenomen opdrachtbeschrijving behoeven verduidelijking?	Voor prijsvergelijkbaarheid en een level playing field moet VRK verduidelijken: verdeling van de circa 1.400 gebruikers, accounts en apparaten van vrijwilligers, scope en frequentie van phishing, vereiste koppelingen, huidige situatie en migratie, talen, contractduur,

Nr.	Vraag	Geanonimiseerde samenvatting van de markt
		supportmodel, gewenste rapportage, maatwerkcontent, toegankelijkheidsniveau, beheerrollen en optionele functionaliteiten.
36	Welke aanvullende aandachtspunten, risico's, innovaties of marktontwikkelingen moeten worden betrokken?	Aanvullend worden genoemd: AI-gegenereerde aanvallen en AI-geletterdheid, transparantie over AI-profilering, realtime begeleiding, fysieke en sociale weerbaarheid, awarenessmoeheid, leverancierscontinuïteit, broncode/data-escrow waar relevant, bereikbaarheid van medewerkers zonder vaste werkplek, hoge in- en uitstroom van vrijwilligers en behoud van historische meetreeksen bij leverancierswissel.

3 Verdere vervolg

Algemeen

De gevolgde marktconsultatie en de deelname daaraan is voor alle betrokken partijen geheel vrijblijvend. Tevens leidt dit op geen enkele wijze tot een overeenkomst en/of enige vorm van juridische binding tussen VRK en de partijen die aan de marktconsultatie hebben deelgenomen. Dit verslag doet geen afbreuk aan deze vrijblijvendheid. VRK is op geen enkele wijze gebonden aan de verkregen informatie en/of de verplichting tot aanbesteding (in welke vorm dan ook) van het onderwerp van de marktconsultatie. VRK bepaalt geheel zelfstandig wat zij met de in deze marktconsultatie verkregen reacties en/of informatie doet.

Vervolgstappen en beoogde planning

VRK gebruikt de komende periode om het onderwerp “Awareness/e-learning platform informatiebeveiliging en privacy” verder intern te evalueren en te bespreken (mede op basis van de reacties en/of informatie die is verkregen vanuit de marktconsultatie). Hierna wordt naar verwachting een aanbestedingstraject opgestart.

Dankwoord

VRK bedankt alle deelnemende partijen voor de door hun ingediende reactie en de door hen gedane inspanningen in deze marktconsultatie.