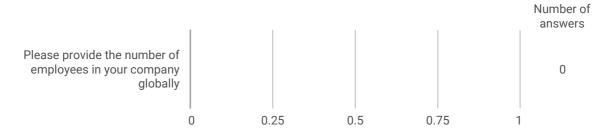
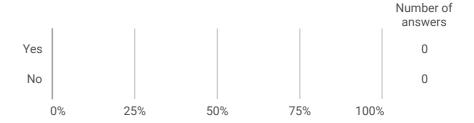
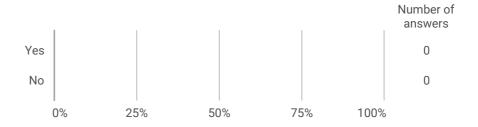
#### Please provide the number of employees in your company globally



Do you have operations/employees in Norway?



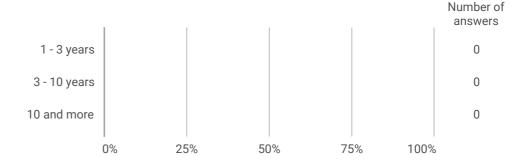
Do you have operations/employees in the European Union/European Economic Area?



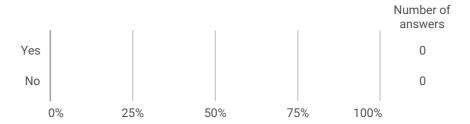
Is your holding company privately held or listed on a stock exchange?



For how many years have your company been in operation?



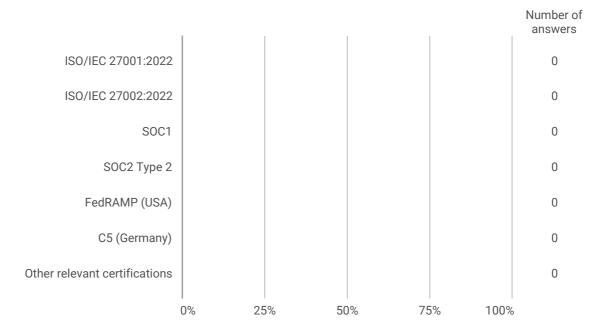
Are you interested in further dialogue/meetings (digital or otherwise) with us regarding the scoped services to the Norwegian public sector (if yes, please double check the email/phone number you provided above is correct)



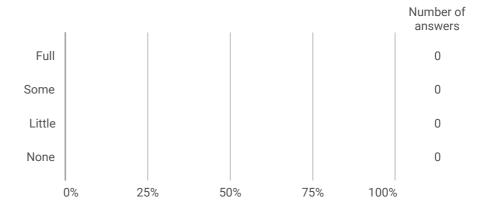
## Please select the features/capabilities your solution offers

					Number of answers
Comprehensive Vulnerability Database					0
Automated Scanning					0
Internal Scanning					0
Vulnerability Prioritization					0
Detailed Reporting and Analysis					0
Integration with SIEMs, Ticketing Systems, etc.					0
Vulnerability Management System					0
Cloud and Container Security Scanning					0
Web Application Scanning					0
API Scanning					0
Threat Intelligence Integration					0
Capability to support GDPR Compliance					0
Capability to support NIS2 Compliance					0
Cloud-based deployment					0
Hybrid deployment					0
On-premises deployment					0
	0% 25	5% 50	0% 75	5% 100%	1

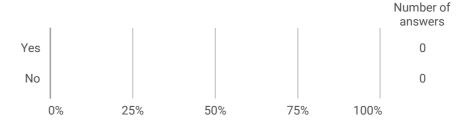
#### Please select the certifications/audit reports your company holds



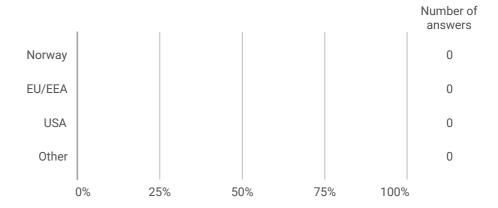
To which extent does your company operate according to the NIST Cyber Security Framework 2.0?



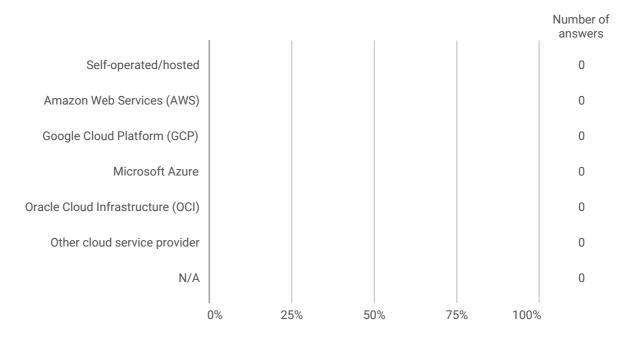
Does your service/tool offer multi-factor authentication (MFA)?



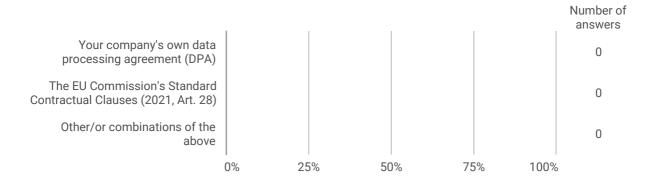
#### Select the location of your primary data centre used to provide your services



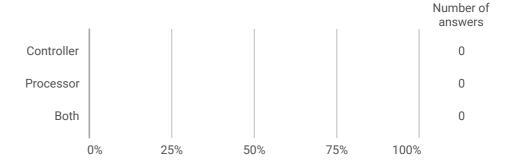
#### How is your primary data centre operated?



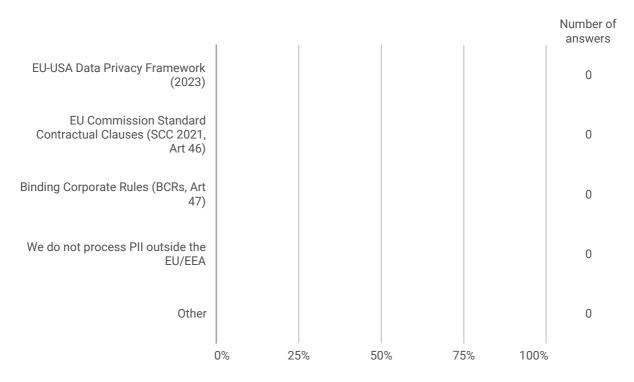
## Under which contract is personally identifiable information (PII) protected in the EU/EEA?



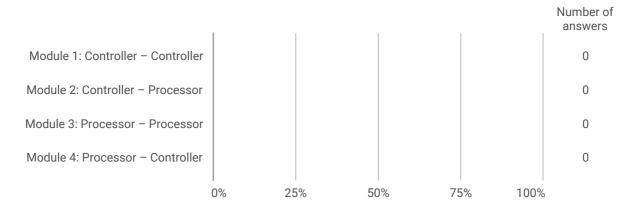
#### Select the role you have when processing PII



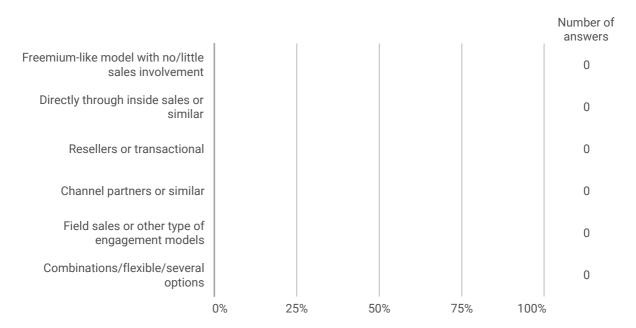
Are you transferring or processing PII outside the EU/EEA? If so, how do you ensure that the "essentially equivalent standards and protections" is provided as required by GDPR?



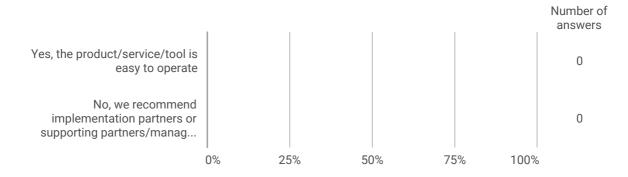
# If you are using SCC (2021, Art 46) for transfers out of the EU/EEA (international transfers) which modules are in use? Select all modules in use



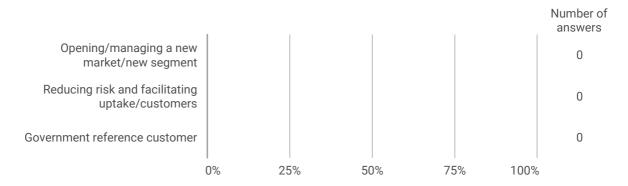
## Do you sell directly or through resellers/channel partners or similar to the public sector?



Is your product/service/tool easy to operate or do you recommend implementation partners or supporting partners/managed services?



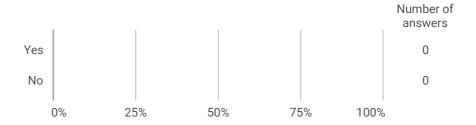
How will a government framework agreement/contract be of interest or benefit to you?



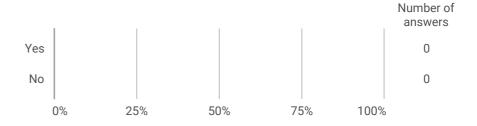
## Select your licensing models

	ı	ı			Number of answers
Perpetual licensing					0
Subscription Enterprise					0
Subscription User-based					0
Volume based/Assets scanned/Other metric					0
Offer several alternatives/flexible/several options					0
Free tiers					0
Pay-as-you-go					0
Open source/free, no other offers					0
Open source/free, paid support or additional features					0
Custom pricing					0
Other/not applicable					0
	0% 2	5% 50	)% 75	5% 100%	

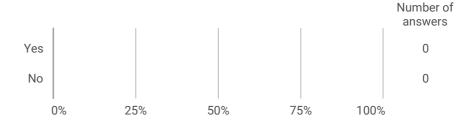
Do you offer special licensing terms/pricing for public sector centrally managed high-volume framework agreements/contracts?



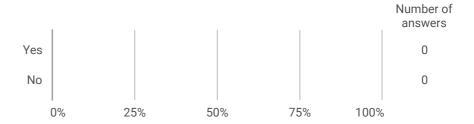
Does your company currently have government entities or public sector entities (globally) as customers?



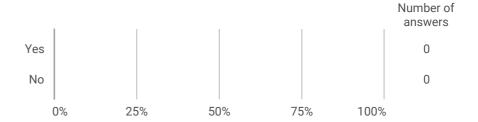
Is your company compliant with all applicable sanctions, regulations and export/import controls from the UN, the United States of America, the European Union and Norway?



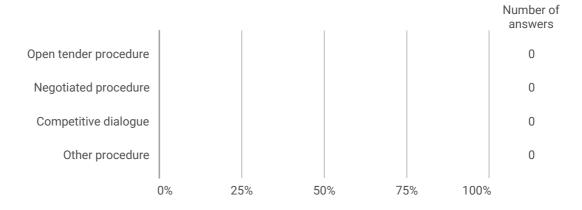
Has your company participated in a procurement procedure in accordance with European Union Procurement Directive 2014/24 previously?



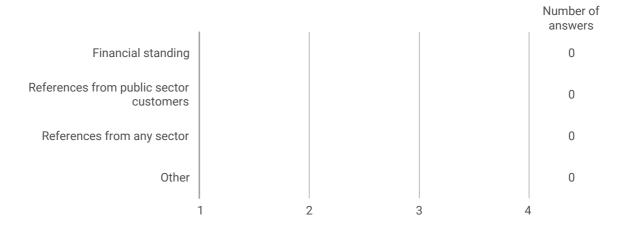
Is your company familiar with the European Single Procurement Document (ESPD)?



In your experience; which type of procurement procedure is preferred?



In which order do you consider the following qualification criteria to be most important/relevant? (1 is most relevant and 5 is least relevant)



# In which order do you consider the following evaluation/award criteria to be most important/relevant? (1 is most relevant and 5 is least relevant)

	ı	ı	I	ı ı	Number of answers
Price					0
Quality/Functionality/Technical aspects					0
Information security/GDPR					0
Climate/Environment/Energy Consumption					0
Contract risk/Legal terms/Licensing					0
	1 2	2 3	3	4 5	

### Which of the other RFIs do you intend to answer?

					Number of answers
N/A					0
Threat Intelligence Platform					0
Third Party Privacy Compliance Management					0
Security Training and Awareness					0
Web Application Firewall					0
Security Governance, Risk and Compliance (Security GRC)					0
Security Incident and Event Management (SIEM)					0
Endpoint Detection & Response (EDR) Platform					0
Vulnerability Scanning					0
	0% 25	5% 50	)% 75	5% 100%	