sikker digital DK

Questionnaire for the IT supplier

	Description of services/solutions	Answers
1.	**What measures do you have in place to protect against unwanted access?**	
A	Where are the servers located and how is access to them controlled? Are they located, e.g., in your own data centre, with a hosting provider or do you use a cloud service?	
B	What best practice security measures, such as firewall, antivirus, encryption, network segmentation and user and access management have you established?	
C	How, and during which periods, do you monitor whether the solution is working and whether there are signs of irregular behaviour? Do you use, e.g., a SIEM or other monitoring solution, and what are your processes?	
D	What procedures do you have for reporting, handling and updating vulnerabilities in your products and solutions?	
	How long after an update is available is it installed?	
E	How is our access to the solution ensured - do you use, e.g., an encrypted connection and multi-factor login?	
2.	**What do you do to ensure availability and high uptime?**	
A	Have you established a redundant solution and what type of redundant solution is it?	
B	What availability does the solution have as a starting point?	
	Is it possible to purchase a higher level of availability?	
C	What procedures do you have for backup and how often are backups carried out?	
	How quickly can data be restored from backup after an incident?	
	How often do you test your backup and when was it last tested?	

	Description of services/solutions	Answers
D	Do you have a contingency plan for how you handle incidents and what does it contain?	
	When was the last time you tested your contingency plan?	
3.	**How do you work with and document your security?**	
A	How have you decided on the security of your solution? Do you use a framework such as, e.g., ISO 27001, OWASP, STRIDE, etc.?	
	Are you certified or do you comply with one of these frames of reference?	
B	How is security audited and tested? Will there be, e.g., penetration tests, third-party audits, code reviews, security reviews conducted, etc.?	
	What methodology does the test follow?	
	How often and in which contexts is your solution tested?	
C	What procedures do you have for risk assessing your solution?	
	How is security thought into the solution?	
D	Do you regularly audit your solution by an external partner, e.g., when preparing an ISAE3402 report and how often is the audit carried out?	
4.	**What do you do to protect personal data?**	
A	Do your services meet the requirements of the GDPR?	
B	How and where do you store data?	
	Do you use any sub-data processors and where are these located?	
	What procedures do you have for deleting data?	
C	How do you ensure that only relevant employees from you have access to data and how is access regulated and monitored?	
	Have these employees signed a confidentiality agreement?	

	Description of services/solutions	Answers
D	How are we notified if there is a breach of security in relation to personal data?	
	How quickly can you guarantee notification after discovery of the breach?	
5.	**What is the division of responsibility between us as a customer and you?**	
A	What requirements and expectations do you have of us as a customer to ensure the overall security of the solution at an appropriate level?	
	What extra services can you offer?	
B	What tasks are we responsible for, e.g., concerning administration and configuration [creating users, decommissioning, managing rights, etc.]?	
C	Are there security elements that can be advantageously implemented to increase the security level? Do you support, e.g., using multi-factor authentication?	