# Spørgeskema til IT-leverandøren

| | Beskrivelse af ydelser/løsninger | Svar |
|---|---|---|
| **1.** | **Hvad gør I for at beskytte mod uønsket adgang?** | |
| **A** | Hvor er serverne placeret og hvordan kontrolleres adgangen til dem? Står de f.eks. i eget datacenter, hos en hosting udbyder eller anvendes en cloud-service? | |
| **B** | Hvilke best practice sikkerhedsforanstaltninger, som f.eks. firewall, antivirus, kryptering, netværkssegmentering og bruger- og adgangsstyring, har I etableret? | |
| **C** | Hvordan, og i hvilke perioder, overvåger I om løsningen fungerer og om der er tegn på uregelmæssig adfærd? Anvendes der f.eks. en SIEM eller anden overvågnings-løsning, og hvad er jeres processer? | |
| **D** | Hvilke procedurer har I for rapportering, håndtering og opdatering af sårbarheder i jeres produkter og løsninger? | |
| | Hvor lang tid efter at der er kommet en opdatering, bliver den installeret? | |
| **E** | Hvordan sikres vores adgang til løsningen – anvendes der f.eks. en krypteret forbindelse og multi-faktor login? | |
| **2.** | **Hvad gør I for at sikre tilgængelighed og høj oppetid?** | |
| **A** | Har I etableret en redundant løsning og hvilken type redundant løsning er der tale om? | |
| **B** | Hvilken tilgængelighed har løsningen som udgangspunkt? | |
| | Er der mulighed for at tilkøbe en højere tilgængelighed? | |
| **C** | Hvilke procedurer har I for backup og hvor ofte bliver der foretaget backup? | |
| | Hvor hurtigt kan data genskabes fra backup efter en hændelse? | |
| | Hvor ofte tester I jeres backup og hvornår er den sidst blevet testet? | |

| | Beskrivelse af ydelser/løsninger | Svar |
|---|---|---|
| D | Har I en beredskabsplan for hvordan I håndterer hændelser og hvad indeholder den? | |
| | Hvornår har I sidst afprøvet jeres beredskabsplan? | |
| **3.** | **Hvordan arbejder I med og dokumenterer jeres sikkerhed?** | |
| A | Hvordan har I taget stilling til sikkerheden i jeres løsning? Anvendes der et rammeværk som f.eks. ISO 27001, OWASP, STRIDE el.lign.? | |
| | Er I certificeret eller efterlever I et af disse rammeværker? | |
| B | Hvordan bliver sikkerheden auditeret og testet? Bliver der f.eks. gennemført penetrationstests, 3. parts audit, codereview, sikkerhedsreview mv.? | |
| | Hvilken metodik følger testen? | |
| | Hvor ofte og i hvilke forbindelser bliver jeres løsning testet? | |
| C | Hvilke procedurer har I for risikovurdering af jeres løsning? | |
| | Hvordan er sikkerhed tænkt ind i løsningen? | |
| D | Får I løbende revideret jeres løsning af en ekstern partner, f.eks. ved udarbejdelse af en ISAE3402 rapport, og hvor ofte udføres revisionen? | |
| **4.** | **Hvad gør I for at passe på persondata?** | |
| A | Lever jeres services op til kravene i GDPR? | |
| B | Hvordan og hvor lagrer I data? | |
| | Anvender I nogle underdatabehandlere og hvor er disse placeret? | |
| | Hvilke procedurer har I for sletning af data? | |
| C | Hvordan sikres det, at kun relevante medarbejdere fra jer har adgang til data og hvordan reguleres og monitoreres adgangen? | |
| | Har disse medarbejdere underskrevet en fortrolighedserklæring? | |

| | Beskrivelse af ydelser/løsninger | Svar |
|---|---|---|
| D | Hvordan bliver vi underrettet, hvis der sker brud på sikkerheden i forhold til persondata? | |
| | Hvor hurtigt kan I garantere underretning efter opdagelse af bruddet? | |
| **5.** | **Hvad er ansvarsfordelingen mellem os som kunde og jer?** | |
| A | Hvilke krav og forventninger har I til os som kunde for at sikre den samlede sikkerhed i løsningen på et passende niveau? | |
| | Hvilke ekstra ydelser kan I tilbyde? | |
| B | Hvilke opgaver står vi for, f.eks. omkring administration og konfiguration (oprettelse af brugere, nedlæggelse, styring af rettigheder osv.)? | |
| C | Er der sikkerhedselementer der med fordel kan implementeres for at øge sikkerhedsniveauet? Understøtter I f.eks. brug af multifaktor loginbeskyttelse? | |