10 spørgsmål om GDPR og IT-sikkerhed din leverandør skal kunne svare på

Det er ved at gå op for de fleste virksomheder, at det er ikke nok, at man som virksomhed har styr på egne datapolitikker, systemer og sikkerhedsprocedurer. Du skal også være helt sikker på, at dine partnere og leverandører har dokumenterede standarder, politikker og procedurer for deres IT-sikkerhed.

Sascha Skydsgaard, CSO, TimeLog

Hovedparten af dine data håndteres ude af huset
De fleste virksomheder har data, der håndteres ude af huset. Det kan være løn- eller bogholderi der er outsourcet, eller bestemte apps eller programmer der tilgås fra skyen. Det betyder, at der er behandling af data i en eller anden form. Derfor er der – som altid når du arbejder med data – risiko for sikkerhedsbrud.

Og uanset om et brud eller uheld sker hos dig eller din leverandør, står du også på mål for sikkerheden.

Flere virksomheder vælger at lade deres arbejde med GDPR og IT-sikkerhed gennemgå og dokumentere af uvildige revisorer. Men uanset om du vælger en leverandør med ISAE-erklæringer eller ej, så skal du aldrig efterlade IT-sikkerheden på perronen.

De ti spørgsmål om GDPR og IT-sikkerhed du skal have svar på
Vi har samlet de essentielle problematikker og spørgsmål til dig, så du kan sikre, at din leverandør overholder GDPR og har sikre procedurer og IT-systemer.

#01 Hvordan dokumenterer I, at I behandler personfølsomme data korrekt?

Medarbejderdata, kundedata mv. håndteres typisk både af jer selv samt jeres leverandører. Men det er din virksomhed, der står til ansvar for, at de behandles korrekt. Derfor skal I bede om dokumentation fra jeres leverandør der beskriver, hvordan de er GDPR-compliant.

#02 Hvilke kontrolmål har I?

Sørg for at spørge ind til hvilke kontrolmål din leverandør har i forhold til datasikkerheden og IT-infrastruktur. En væsentlig del af ISAE 3402 er at opsætte en række dokumenterede kontrolmål, som herefter efterses af et specialiseret revisionshus. Et kontrolmål kan fx være at etablere et ledelsesmæssigt grundlag for at kunne igangsætte og styre implementeringen og driften at informationssikkerhed i organisationen.

#03 Hvornår fik I senest gennemgået jeres IT-compliance?

Spørg din leverandør hvor ofte de reviderer, validerer og opdaterer deres IT-politik og sikkerhed. I virksomheder kommer der konstant nye programmer, IT-værktøjer eller apps til – og det skal afspejles i processer samt dokumentationen.

Det er ikke nok, at en leverandør har lavet en IT-politik tilbage i 2018, da GDPR-forordningen blev indført. Den skal hele tiden opdateres. Til forskel fra fx ISO 2700X-certificeringen varetages kontrollen af ISAE 3402 og ISAE 3000 hvert år. En ISO 2700X-certificering ikke skal fornyes, men er et stempel på, at forholdene på tidspunktet for certificeringen er i orden. Så hvis en leverandør har en ISO-certificering, så spørg om, hvornår den er anskaffet.

#04 Reviderer I både processer og procedurer samt fysisk og logistisk sikkerhed?

Hvor ofte kommer du forbi din leverandør? Er de placeret helt eller delvist i et andet land? En ISAE 3402 erklæring inkluderer også en fysisk revision af sikkerheden.

#05 Hvordan er jeres procedure for håndtering af personfølsomme data?

Før du implementerer et nyt system i din virksomhed, så skal du kende hele processen for, hvordan din leverandør behandler dine, dine kunders eller medarbejderes data. I Europa er alle virksomheder underlagt de samme regler i forhold til GDPR, så det er mere dokumentation af hvordan virksomheden lever op til reglerne, du skal være opmærksom på.

#06 Hvad er jeres fremgangsmåde i tilfælde af et sikkerhedsbrud?

Spørg hvordan leverandøren håndterer et brud på sikkerheden. Og læg mærke til om de har en standardiseret proces; naturligvis dokumenteret.

Er jeres data for eksempel er blevet tilgået af nogen, der ikke har tilladelse til det, har din leverandør pligt til at informere dig. Det er dog først med en ISAE 3000 erklæring, at du er garanteret, at dette sker. Det skyldes, at der er – når man skal opnå en ISAE 3000 erklæring – bliver opsat en procedure, og denne gennemgås regelmæssigt.

#07 Hvilke data håndterer I?

Du har sikkert en god ide om, hvilke data din leverandør burde håndtere. Men sørg for, at din leverandør kan dokumentere alle de data, de håndterer; også hvis din leverandør har underleverandører eller partnere. Med en ISAE 3000-erklæring kan du se en præcis opgørelse af hvilke data, der håndteres. Dermed slipper du for selv at undersøge det.

#08

Hvilke risici har I afdækket i forbindelse med håndtering af mine data?

Det er altid godt at være forberedt. Så før du indgår samarbejde med en ny leverandør, skal du bede om en udførlig beskrivelse af, hvilke risici leverandøren har oplistet i forbindelse med håndtering af data.
Med ISAE 3402 får du vished for, at processer og procedurer omkring data er gennemgået af en uvildig specialist samt kontrolleret.

#09

Hvordan har I sikret, at der er samspil mellem jeres IT-sikkerhed og GDPR-forpligtelser?

Mange virksomheder er relativt gode til at beskrive, hvordan de håndterer reglerne i GDPR. Det er dog mindst lige så vigtigt, at IT-sikkerheden – det vil sige fx systemer, infrastruktur og processer – fungerer i samspil med GDPR, og at IT-sikkerheden er lige så vel dokumenteret som selve GDPR-politikken.
Uden IT-sikkerhed har GDPR tiltag ikke meget værdi. Vil du være på den sikre side, så kig efter en leverandør med både en erklæring om ISAE 3000 samt ISAE 3402.

#10

Hvordan dokumenterer I, at IT-sikkerheden i jeres virksomhed hele tiden modnes og løbende forbedres?

Du vil gerne vide, at du har en leverandør, hvor sikkerhed ikke bare er et modeord, men hvor det er en integreret del af organisationen. Som en del af ISAE 3402 er det et krav, at der er intern uddannelse om IT-sikkerhed, behandling af data mv. Så spørg din næste leverandør, hvad de gør for at sikre, at medarbejdere også tænker IT-sikkerhed og GDPR ind i deres arbejdsrutiner.

Kort **om TimeLog**

TimeLog hjælper konsulent- og rådgivningsvirksomheder med at udvikle forretningen.

Grundlagt i 2001 af to danske entreprenører

+60 glade TimeLoggere

Har både ISAE 3000 GDPR og ISAE 3402 revisorerklæringer

Kunder i +15 lande

+800 kunder

Kundestørrelse: 1-1.700 brugere

Hvis du har spørgsmål, kommentarer eller vil vide mere om TimeLog, er du naturligvis velkommen til at kontakte os:

TimeLog A/S
Vesterbrogade 149, bygn. 4, 1.
1620 København V
info@timelog.dk
+45 70 200 645

www.timelog.com/da