”Jamen, vi har jo vores egen lukkede ChatGPT, så vi er vel på den sikre side...?!”

Lukkede AI-systemer fritager ikke virksomheden fra complianceregler og –forpligtelser. Virksomheder, der benytter egne interne AI-systemer, skal stadig foretage risikovurderinger, fastlægge behandlingsgrundlag, føre kontrol med leverandører og overholde øvrige krav i AI-forordningen, GDPR og lignende compliancelovgivning.

Mange virksomheder bruger deres egne, lukkede chatbots og AI-systemer og tror (fejlagtigt), at de undgår compliancekrav og AI-forordningens forpligtelser ved kun at bruge systemet internt.

Dette er dog ikke korrekt.

Selv ved brug af lukkede systemer kan virksomheden risikere sanktioner, hvis reglerne for korrekt anvendelse af AI ikke overholdes. Databeskyttelsesregler og øvrige compliancekrav gælder også for virksomheders interne behandlinger, og AI-forordningen tager udgangspunkt i systemets risikoprofil – ikke i, om systemet er lukket eller ej.

Der er altså flere faldgruber, man skal være opmærksom på for at undgå sanktioner, uanset hvilket AI-system der benyttes.

AI-forordningens fokus på risikoprofilen

AI-forordningen baserer sine krav på en risikobaseret tilgang. Det betyder, at det ikke er afgørende, om en virksomheds AI-system er lukket eller ej, men derimod, hvilken risiko systemet udgør for brugere, medarbejdere eller samfundet generelt.

Hvis et lukket system eksempelvis benyttes til beslutningstagning om ansættelser eller interne evalueringer, kan det stadig falde ind under højrisikokategorien i AI-forordningen, og de forpligtelser, der følger med et sådant system.

En virksomhed, der anvender et AI-system som led i sine interne arbejdsprocesser, vil desuden som udgangspunkt blive anset for at være ”idriftsætter” efter AI-forordningens definition. At være idriftsætter kan i sig selv medføre forpligtelser for virksomheden, uanset hvilken type AI-system der benyttes.

Øvrige compliancekrav

Virksomheders brug af AI-systemer medfører derudover ofte andre compliancekrav og forpligtelser. Mange virksomheder har en opfattelse af, at de kan undgå at skulle forholde sig til særligt GDPR-reglerne om behandling af personoplysninger, hvis de anvender lukkede AI-systemer, hvor data kun deles inden for virksomheden. Dette er imidlertid en misforståelse.

GDPR gælder også ved interne, lukkede behandlinger af personoplysninger, hvilket betyder, at virksomheder fortsat skal sikre, at behandlingen sker i overensstemmelse med GDPR-reglerne, når der behandles personoplysninger i egne AI-systemer.

Behandling af personoplysninger kræver eksempelvis, at virksomheden efterlever GDPR-reglerne vedrørende behandlingsgrundlag, oplysningspligt og sikkerhedsforanstaltninger. Virksomheden er altså ikke på den sikre side, bare fordi AI-systemet scorer lavt på risikobarometeret.

Endelig er det særligt relevant for virksomheden at foretage en grundig vurdering af de risici, der er forbundet med brugen af AI-systemet. Dette indebærer blandt andet en vurdering af, hvorvidt systemet behandler anonyme data eller ej, og selv hvis systemet opererer med anonyme data, skal det undersøges, hvordan AI-modellen er trænet – herunder om der er anvendt personoplysninger som input-data under træningen – og hvilke konsekvenser dette kan have for databeskyttelsen. Det er dermed også afgørende, at virksomheden foretager en grundig due diligence på sine leverandører for at kunne leve op til gældende complianceregler.

Virksomheder skal altså foretage en grundig vurdering af deres lukkede AI-løsninger og sikre, at alle aktiviteter også lever op til GDPR-reglerne.

Hvordan kan vi hjælpe?

Hos NJORD Law Firm hjælper vi dig med at forstå, hvordan brugen af et AI-system påvirker din virksomhed. Vi tilbyder rådgivning om, hvilke krav og forpligtelser din virksomhed er underlagt, både efter AI-forordningen men også øvrige compliancekrav, og vi bistår med, hvad I skal implementere for at efterleve dem.

NIELS SKYTTEDAL DAHL-NIELSEN
ADVOKAT, PARTNER

(+45) 40 30 97 49
NDN@NJORDLAW.COM