Rådet for Digital Sikkerhed

23. oktober 2017

Rådet for Digital Sikkerheds høringssvar til Udkast til bekendtgørelse om visse regler om prøver og eksamen i de gymnasiale uddannelser

Rådet for Digital Sikkerhed (RfDS) har noteret sig høringen om ovenstående udkast til Betænkning. RfDS har adresseret de forhold i Betænkningen som vedrører behandling af personoplysninger og har i den forbindelse nedenstående bemærkninger.

Baggrund

RfDS har noteret sig at Betænkningens § 5, stk. 3 lægger op til, at der kan fastsættes regler om "brug af cloud-tjenester, overvågning og logning af netværksaktivitet, monitorering af elevernes computere/tablets mv. og brug af elektroniske enheder i øvrigt".

Af § 6, stk. 4 og 5 fremgår det videre, at bekendtgørelsen har til formål at tage hånd om situationer, hvor adgang til internettet i bred forstand ikke er tilladt, men hvor der kan være behov for alligevel at hente bestemte ting på internettet, evt. fordi det ikke kan opbevares lokalt.

Af § 6, stk. 6 fremgår det så at "Det er en forudsætning for, at eksaminanden kan anvende digitale hjælpemidler, herunder computere, ved prøven, at eksaminanden giver institutionen adgang til at undersøge de anvendte hjælpemidlers indhold, søgehistorik, logfiler mv. samt eksaminandens anvendelse af materialer, konti på sociale medier mv. på internettet med henblik på udredning af formodning om snyd eller andre brud på eksamensreglerne. Hvis eksaminanden ikke opfylder denne forudsætning, kan institutionen beslutte at iværksætte en sanktion i henhold til bekendtgørelse om studie- og ordensregler m.v. i de gymnasiale uddannelser."

Bekendtgørelsen er et invasivt indgreb i privatlivet

RfDS bemærker indledningsvist, at der synes at være tale om et meget invasivt indgreb i eksaminandernes ret til privatlivets fred. Ved at undersøge hjælpemidlernes indhold, ved at gennemgå søgehistorik og logfiler og ved at skaffe sig adgang til sociale medier og evt. andre tjenester på nettet, som eksaminanderne måtte gøre brug af, vil de gymnasiale institutioner få adgang til eksaminandernes følsomme personoplysninger. Med andre ord er der stor risiko for, at de gymnasiale institutioner med stor sandsynlighed få adgang til oplysninger om politiske holdninger, religiøse holdninger, helbredsoplysninger og seksuelle oplysninger.

Der er også risiko for, at der gives adgang til almindelige personoplysninger om andre rent private forhold, som eksaminanderne ønsker at betragte som fortrolige; f.eks. dagbøger og kommunikation med venner og familiemedlemmer. Endelig er der risiko for, at de gymnasiale institutioner vil få adgang til oplysninger om strafbare forhold; f.eks. oplysninger om software uden licens, materialer som er omfattet af krænkelse af ophavsretten eller ulovlig brug af rusmidler.

Rådet for Digital Sikkerhed
Axeltorv 6, 3. th., 1609 København V
Telefon: +45 29 23 70 00 mail: info@digitalsikkerhed.dk web: www.digitalsikkerhed.dk

Der er med andre ord tale om adgang til oplysninger som er er fundet beskyttelsesværdige i f.eks. Den europæiske unions charter om grundliggende rettigheder, artikel 8 og forordningen 2016/679 (persondataforordningen). Selv om der ofte kan gives adgang til sådanne oplysninger i medfør af lov, bør der lægges vægt på grundlæggende principper for beskyttelse som f.eks. lovlighed, rimelighed og gennemsigtighed, formålsbegrænsning, dataminimering, rigtighed, opbevaringsbegrænsning, integritet og fortrolighed samt ansvarlighed. Bekendtgørelsen synes især at være udfordret i forhold til rimelighed og dataminimering. Indgrebet synes simpelthen ikke at være proportionalt, og desuden vil der blive behandlet masser af personoplysninger, som ikke er nødvendige for formålet.

Omgåelse af reglerne

RfDS bemærker desuden, at eksaminanden med lidt teknisk snilde forholdsvist uproblematisk vil kunne omgå intensionerne med Bekendtgørelsen. Det vil f.eks. være muligt at kryptere filer lokalt på terminalernes diske og dermed gøre dem utilgængelige for de gymnasiale institutioner. Desuden kan eksaminanderne placere dem på steder på disken, hvor de kun vanskeligt lader sig finde. Hvad angår selve kommunikationen kan eksaminanden anvende krypterede forbindelser f.eks. https eller VPN til at sløre trafikkens indhold. Der kan også anvendes onion-routing i form af f.eks. TOR-browseren; ligeledes med det formål at sløre trafikken. Endelig vil eksaminanden være lokal administrator på sit terminaludstyr, hvorfor der kan manipuleres med logs; herunder foretages sletningen af loggen.

Den smarte eksaminand vil derfor have mulighed for at omgå Bekendtgørelsens intension. Ligesom man altid har kunne snyde ved at skrive noter på maven og læse disse, mens man gik på toilettet, kan man også snyde i den digitale verden. Men det centrale er, hvor grænsen for invasive tiltag i forhold til at imødegå snyd skal være. I dette tilfælde er grænsen klart overtrådt, fordi de invasive tiltag er meget vidtgående især henset til den store mængde af eksaminander, som ikke snyder.

Alternative løsninger

I stedet for at etablere invasive tiltag i form af gennemgang af eksaminandens personoplysninger bør de gymnasiale institutioner etablere andre (til dels tekniske) tiltag for at løse problemet. De gymnasiale institutioner kan f.eks. kigge på nogle af de løsninger, der allerede er taget i brug på universiteterne.

RfDS står naturligvis til rådighed for en uddybelse af ovenstående bemærkninger.

Med venlig hilsen

Bestyrelsen
Rådet for Digital Sikkerhed