BØRNE- OG UNDERVISNINGSMINISTERIET
STYRELSEN FOR IT OG LÆRING

Tjekliste — Anvendelse af gratis tredjepartsapps og -værktøjer

Hvis apps, programmer og andre værktøjer kan anvendes uden betaling, er der risiko for, at betalingen sker ved at benytte sig af data om dig, dine kolleger eller dem du underviser til analyse- og marketingformål. Derfor bør du nøje overveje, hvorvidt der er behov for værktøjerne samt brugen heraf, førend du beder nogen anvende hjemmesider og evt. installerer gratis apps på deres egne eller skolens devices. Finder du alligevel, at der er et undervisningsmæssigt behov for at anvende det pågældende værktøj eller app, har Børne- og Undervisningsministeriet udviklet en tjekliste til at understøtte din vurdering af, hvorvidt det er forsvarligt at bruge.

Tjeklisten stiller en række spørgsmål og uddyber den tilknyttede risiko, og det anbefales, at du noterer et svar ud fra hvert spørgsmål, og gemmer resultatet et sted som dokumentation for beslutningen om at anvende værktøjet eller appen. Tjeklisten er tiltænkt it-vejledere, andre it-fagpersoner og skoleledere i undervisningssektoren. Er du i tvivl, bør du gå til forvaltningen eller til kommunens eller institutionens databeskyttelsesrådgiver (DPO) for at sikre, at du overholder regler om persondatabeskyttelse.

Tjekliste — den hurtige vurdering

Spørgsmål	Risiko	Egne noter
Skal der angives personlige oplysninger for at bruge produktet? Personlig data er eksempelvis navn, fødselsdato, billede, e-mailadresse mv.	Hvis det er nødvendigt at brugeren angiver mange personoplysninger, bør man overveje, om det er forsvarligt at bruge produktet. Anmodes der eksempelvis kun om navn og e-mail, kan man vælge at anvende et neutralt navn/alias (fx Bruger01, Bruger02 mv.) kombineret med brugerens skole/institutions-mail. Vær dog opmærksom på, at det kan stride mod nogle produkters retningslinjer for anvendelse.	
Indeholder produktet reklamer?	Apps og hjemmesider, som indeholder reklamer, indsamler ofte personlig information om brugerne og profilerer dem (browser fingerprint) baseret på, hvordan de bruger appen eller hjemmesiden. Det udsætter brugerne for en privatlivsrisiko, og man bør derfor nøje overveje, om det er forsvarligt at anvende appen i en undervisningssammenhæng. I flere browsere er det muligt at installere plugins, som anonymiserer brugerens færden, og fx Firefox tilbyder sporingsfri færden på nettet: https://www.mozilla.org/da/firefox/features/private-browsing/	

(Kun relevant ift. apps) Hvilke tilladelser beder appen om ved installation og brug?	Nogle apps beder om mange tilladelser, førend de kan køre. Der kan være tale om tilladelse til at se kontaktliste, bruge mikrofon, kamera eller se lokation. Overvej derfor grundigt om de tilladelser, som produktet anmoder om, stemmer overens med produktets funktion. Eksempelvis har en algebra-app næppe grund til at have adgang til lokation og kontaktliste. Lav gerne en gennemgang af tilladelser inden ibrugtagning af appen, hvor alle ikke nødvendige tilladelser slås fra. Der er hjælp at hente i værktøjet "Appcensus", som introduceres i bunden af tjeklisten. På Google Play Store angives det under beskrivelsen af hver app, hvilke tilladelser den anmoder om.	
Bruges der tredjeparts cookies?	Hvis man logger på med sin Facebook-, Google- eller Microsoft-konto, kan disse platforme også få adgang til data om hvordan man bruger det pågældende værktøj. Den viden kan blandt andet bruges til markedsføringsformål. Det kan være problematisk, hvis værktøjet registrerer mange typer personoplysninger om brugeren. Det anbefales, at man ikke logger på med sine private SoMe-profiler. Der er hjælp at hente i værktøjet "Exodus Database," som introduceres i bunden af tjeklisten.	
Er det nødvendigt at oprette sig med mail, for at benytte sig af produktet?	Hvis skolen/institutionen ikke stiller e-mail til rådighed, kan deltagerne i undervisningen have svært ved at anvende produktet. De kan oprette sig i et af de gratis e-mail alternativer, som dog anvender data til markedsførings- og analysebrug, hvorfor det også bør overvejes, om det er fornuftigt. Derudover tillader mange mailleverandører ikke, at børn under 13 opretter sig i deres systemer.	

Tjekliste — Den grundigere vurdering (forsættelse af den hurtige)

Spørgsmål	Risiko	Egne noter
Gemmer appen eller hjemmesiden informationer, opgaver og anden data?	Er det tilfældet, er det vigtigt at finde ud af, hvem der får kontrol med data, og om det er muligt at trække data ud af appen eller hjemmesiden og herefter slette det i appen eller hjemmesiden, når den ikke længere skal bruges. Hvis leverandøren bliver ejer af data, kan det ikke anbefales at anvende produktet til noget, som ikke kan tåle at blive delt offentligt.	
Er leverandøren bag produktet fra et EU-land eller ej?	Virksomheder i EU-lande skal overholde GDPR, hvilket stiller strengere krav til databeskyttelsen i produktet. Hvis virksomheden ikke er beliggende i EU/EØS, kan I tjekke på Datatilsynets hjemmeside, om virksomheden er på listen over godkendte tredjelande. Er landet ikke på listen over godkendte tredjelande (USA betragtes fx som et usikkert tredjeland), kan man ikke være sikker på, at tjenesten giver de registrerede en tilstrækkelig beskyttelse. Man bør derfor overveje, hvordan man kan anvende det gratis produkt ved at registrere så få personhenførbare oplysninger som muligt.	

Hvordan og hvornår bliver data slettet?	Personoplysninger må kun opbevares i den periode, det er nødvendigt til opfyldelse af det formål, hvortil de blev indsamlet. Derfor skal man som underviser opfordre til at alle sletter profilen, når værktøjet ikke længere bruges i undervisningen.	
Hvordan foregår sociale interaktioner?	I nogle apps kan brugere kontakte hinanden frit og uden, at interaktion og deling af informationer overvåges af eksempelvis moderatorer. Undersøg derfor nøje, hvordan det foregår i den pågældende app, og overvej om især yngre elever, bør udsættes for denne risiko.	
Viser produktet personlig data offentligt?	I nogen produkter bliver man bedt om at oprette en profil, og til tider vil information som eksempelvis navn, køn, alder og land/by blive vist offentligt, uden det kan slås fra. Overvej derfor at anonymisere personlig data fx med initialer eller at angive lokation som "Danmark" i stedet for en specifik by.	
Har virksomheden en privatlivspolitik eller betingelser for brug?	Hvis betingelserne er til at forstå for almindelige mennesker, så har virksomheden bag højest sandsynligt også overvejet, hvordan den håndterer data. Er den derimod overordentligt lang og kompliceret skrevet, kan det være et tegn på, at virksomheden forsøger at skjule deres uetiske anvendelse af din data. Brug evt. https://tosdr.org/#services til at vurdere produktets privatlivspolitik.	

En række organisationerne har udviklet værktøjer, der kan bruges til at understøtte den kritiske evaluering af produkterne inden anvendelse. Værktøjerne kommer fra tredjeparter, som har en kritisk tilgang til privatliv i digitale produkter. Børne- og Undervisningsministeriet har ikke samarbejde med de pågældende organisationer og har ikke screenet alle deres vurderinger. De kan derfor anvendes på eget ansvar.

- **AppCensus** har vurderet en lang række gratis Android apps og rapporterer på, hvorvidt de tilgår og deler personoplysninger med andre parter. Deres vurdering er tilgængelig her: https://search.appcensus.io/
- **Exodus** analyserer applikationer fra Android og lister de tredjepartscookies, som appen anvender. En tredjepartscookie er et stykke software, som indsamler data om dig og din brug af en applikation og som deles med andre end dem, der har udviklet applikationen. Analyserne tilgås her: https://exodus-privacy.eu.org/en/
- **Commonsense.org** udarbejder privatlivsevalueringer på en lang række gratis apps, som typisk er målrettet undervisningssektoren i USA. Evalueringerne er designet til at understøtte skoler og undervisere i at tage informerede beslutninger om den potentielle privatlivsrisiko forbundet med brugen af applikationerne. Evalueringerne tilgås her: https://privacy.commonsense.org/evaluations/1