



DPO Rapport for FGU Danmark

Indledning

Denne rapport er udarbejdet med henblik på at informere ledelserne hos FGU-institutioner i Danmark samt interne og eksterne interessenter om status på arbejdet med overholdelse af databeskyttelsesreglerne - som fastlagt i EU Databeskyttelsesforordningen (i det efterfølgende benævnt som GDPR) (EU 2016/679) samt i de danske vedtagne bestemmelser om samme (databeskyttelsesloven nr. 502 af 23/05/2018).

Cybersikkerhed

Bl.a. Danmarks rolle i den Europæiske håndtering af konflikten mellem Rusland og Ukraine, har for alvor sat Danmark på landkortet hos de cyberkriminelle, hvor både de almindelige kriminelle elementer samt statsstyrede enheder har forsøgt at angribe organisationer i Danmark. Vi har set uautoriserede droner, der har lukket vores lufthavne, vi har set flere statslige og kommunale hjemmesider blive lagt ned og vores Statsminister har endda udtalt, at Danmark sammen med resten af EU er i hybridkrig med Rusland.

Forsvarets Efterretningstjeneste (FE) har i sin risikovurdering beskrevet, at Rusland er en betydelig trussel, og at Rusland fører en *hybridkrig* mod Danmark og NATO, hvor cyberangreb, sabotage og provokationer indgår som centrale elementer. FE fremhæver jamming af GPS-signaler, simulerede angreb og hensynsløs sejlads som eksempler. Destruktive cyberangreb mod kritisk infrastruktur er en reel mulighed, især som led i en destabilisering af Danmark.

Center for Cybersikkerhed meddeler, at Cybertruslen mod Danmark er alvorlig, og at vi oplever det mest komplekse trusselsbillede siden 2. verdenskrig.

Trusselsniveauer fordelt på angrebstype ifølge CfCS:

- **Cyberkriminalitet: Meget høj** (ransomware er den største enkelttrussel).
- **Cyberspionage: Meget høj** (statslige aktører, især Rusland og Kina).
- **Cyberaktivisme: Høj** (pro-russiske grupper udfører DDoS-angreb mod myndigheder og virksomheder).
- **Destruktive cyberangreb: Middel** (primært fra statslige aktører som Rusland).
- **Cyberterror: Ingen** (ekstremister har ikke kapacitet).

FGU Danmark

01-01-2026

Ny Vestergade 17, 2. sal
1471 København K.

Tlf. 3044 4033

Mail: fgu@fgu.dk

www.fgu.dk

CVR: 40842357

Måske derfor blev 2025 året, hvor vi i FGU for alvor første gang mærkede truslen fra de cyberkriminelle. Vi har været udsat for CFO-fraud og Phishing angreb, hvor de kriminelle elementer havde held til at fravriste FGU-institutionerne et mindre beløb, der dog var stort nok, til at det var ærgerligt.

Der er ingen tvivl om, at truslen fra de cyberkriminelle er i stærk stigning, og vi kan i det kommende år forvente mange flere forsøg fra disse elementer, hvor de forsøger at svindle sig til en fortjeneste på vores bekostning.

For alle i FGU har det derfor aldrig været vigtigere end lige nu, at vi er skeptiske og årvågne og ekstra opmærksomme på, at vi ikke risikerer at falde i en fælde, sat af en ondsindet aktør. Vi skal fortsætte det gode arbejde med at uddanne vores medarbejdere i at forsvare og skærme mod cyberangreb, uanset i hvilken forklædning den måtte komme. I Mindzeed, vil vi i det kommende år fortsat have stor fokus på cybersikkerhed – mere end på GDPR, hvor jeg oplever, at vi har et solidt vidensniveau i FGU.

Til orientering vil i perioden 1. december til 30. juni køre flere Phishingkampagner rettet mod organisationens medarbejdere, for at teste vores fælles modstandsstyrke og evne til at identificere forsøg på at snyde sig til informationer eller penge. Disse kampagner vil være udfærdiget af en samarbejdspartner, der har stor erfaring indenfor området. Resultaterne vil blive anonymiserede og hver enkelt institution vil få oplyst, hvor mange der i givet fald er faldet for vores svindel, men det vil ikke blive oplyst, hvilke personer det drejer sig om.

Sikkerhedsbrud

Vi har i 2025 oplevet et antal sikkerhedsbrud nogenlunde på niveau med 2024. De fleste skyldtes menneskelige fejl, som resultat af travlhed eller manglende omtanke, hvor alle involverede efterfølgende er blevet klar over, at der blev begået en fejl, lærte af det, justerede proceduren og helt sikkert ikke vil gentage samme fejl.

Nogle få sikkerhedsbrud blev påført os udefra. Heldigvis uden de har haft nævneværdige konsekvenser.

Her ud over har vi været udsat for flere Phishing-angreb, hvilket endnu ikke ført til alvorlige konsekvenser for de involverede. Men blot understreger, at hvis ikke vi konstant er opmærksomme og skeptiske, vil der komme tilfælde, der på et tidspunkt vi få alvorlige konsekvenser for den enkelte.

Som nævnt lever vi i en verden, hvor risikoniveauet for cyberangreb i Danmark til stadighed er meget højt og stigende. Derfor er det nødvendigt,

at vi alle bidrager til at højne det daglige forsvar, ved at udvise skepsis og omhu i brugen af IT-udstyr, og vi kan desværre ikke have blind tillid til selv den mest troværdige partner.

Hackerne er aldrig længere væk end et klik på det forkerte link.

Kunstig intelligens - AI

Anvendelsen af kunstig intelligens (AI), fortsætter sin indtog i hverdagen, både i forhold til FGU's kerneopgave – undervisningen, men så sandelig også i andre områder af vores hverdag. Vi ser en konstant syndflod af nye AI-produkter skylle ind over os, både som selvstændige produkter, hvilket i sig selv er en udfordring, men endnu mere udfordrende ser flere produkter og services fra vores databehandlere, hvor AI bliver indlejrede funktioner i disse produkter. Det er derfor vigtigere end nogen sinde, at vi tager aktiv stilling til, hvor meget AI skal have lov til at fylde i vores hverdag og på hvilken måde, i hvilket omfang samt ikke mindst hvilke kompetencer vores egen organisation skal besidde for at arbejde med denne teknologi på betrykkende måde og sidst men ikke mindst skal forholde os kritisk til de produkter, vi påtænker at tage i anvendelse.

AI i FGU sektoren

Der udarbejdet et sæt dokumenter med vejledninger til FGU-Institutionerne og deres ledelse. Alt ligger tilgængelig på TEAMS og materialet omfatter:

- AI Guide – målrettet til undervisere og vejledere
- En AI Produktoversigt
- Anbefaling til anvendelse af AI i FGU
- Guide til FGU-ledelser om ansvarlig brug af generativ AI
- En hjemmesidetekst målrettet elever
- En gennemgang af forskellen mellem intern vs ekstern AI
- Oversigt over lovgivning og dokumentationer
- Pixiebog om GDPR-sikkerhed
- Pixiebog om brug af fotos

Desuden har jeg, udarbejdet en skabelon til en mere detaljeret risikovurdering af et AI-produkt eller en service man påtænker og jeg står selvfølgelig til rådighed, hvis man vil benytte dette værktøj.

Vi vil løbende underrette institutionerne om anbefalinger i udnyttelse af kunstig intelligens.

For de som ønsker adgang til materialet, skal man blot sende en mail til iso@fgu.dk

NCIS - webfiltrering

I dette efterår besluttede regeringen at der skal indføres en aktiv filtrering af de websider vore elever kan tilgå via FGU's netværk. Vi har i skrivende stund desværre ikke kunnet få et oplæg fra Statens IT til, hvordan vi på de 23 af vores institutioner, der er tilknyttet Statens IT, kan implementere en efterlevning af denne lovgivning. De mangler ressourcer til at besvare vores henvendelse, hvilket kan bekymre, når der er vedtaget besparelser, der betyder endnu færre ressourcer hos Statens IT. Hvor efterlader det FGU-sektoren?

De øvrige 4 institutioner der varetager deres egen IT-drift og dermed ikke er afhængige af Statens IT, er i fuld gang med deres individuelle implementeringsforløb.

Vores uddannelsesplatform

Alle 27 FGU-institutioner er kontinuerligt i gang med at uddanne medarbejderne via vores uddannelsesplatform, hvor vægten som tidligere nævnt er lagt på cybersikkerhed og hvert kursusforløb er tilrettet den enkelte medarbejders jobfunktion, således uddannelsen er mest mulig relevant i forhold til de daglige opgaver.

I skrivende stund pågår et Proof of Concept (POC) hos FGU Kolding Vejen med det formål at få testet behovet for- og kvaliteten af et produkt til scanning af medarbejdernes filer for indhold af persondata, der burde være arkiveret andre steder. Når POC'en er slut, vil vi lave en vurdering af om, vi i det hele taget har behov for sådan et produkt.

Tilbud om uddannelse af bestyrelsesmedlemmer

Med tanke på den øgede risiko for at Institutionerne kan blive udsat for cyberangreb, har bestyrelserne således fået yderligere et område at skulle forholde sig til, når det gælder fordeling af ressourcer. En enkelt bestyrelse har taget mod tilbuddet om uddannelse via vores uddannelsesplatform. Desuden har to bestyrelser taget mod tilbuddet om en introduktion til cyberkriminalitet, og hvordan man som bestyrelse bør forholde sig. For de bestyrelser der ønsker et cyberseminar i det nye år, skal I blot række ud til jeres DPO.

IT-sikkerhedsudvalg under STIL (LISSI)

[I LISSI \(Ledernetværk om informationssikkerhed på selvejende institutioner\)](#)

har jeg sammen med repræsentanter fra forskellige selvejende uddannelsesinstitutioner arbejdet med udviklingen af oplæg til et rammeværk, der har til formål at øge informationssikkerheden generelt i uddannelsessektoren.

I første omgang har man valgt at fokusere på følgende områder:

- [Informationssikkerhedsstandard for selvejende institutioner i Danmark](#)
- Udnyttelse af kunstig intelligens

Vi fortsætter samarbejdet i LISSI i det kommende år og arbejder kontinuerligt på at øge sikkerheden indenfor de selvejende uddannelsesinstitutioner.

Årets FGU Projekter

Der har i årets løb været en del forskellige projekter, hvor jeg som DPO har været involveret.

Jeg vil ikke gennemgå disse i detaljer, blot give en kort oversigt over de væsentligste:

- Udarbejde databehandleraftaler for de institutionerne
 - Gennemgå nye databehandleraftaler med leverandører
 - Review af compliance dokumenterne
 - Udarbejde dokumenter til vejledning om udnyttelse af kunstig intelligens
 - IT-Sikkerhedsudvalget LISSI under STIL, et igangværende arbejde om øget datasikkerhed
 - Mindzeed, vores uddannelsesplatform, igangsætning af nye medarbejdere
 - Løbende deltagelse i statusmøde mellem Statens IT og institutionerne om fremdrift i problemløsning.
 - Kortlægning af leverandørtilfredshed med Statens IT
 - Løbende assistance i forbindelse med sekretariatsopgaver
 - Gennemgå krav til webfiltrering
 - Planlægning af kommende Phishingkampagne
 - Rådgivning af Institutionerne i forhold til daglige spørgsmål relateret til lovgivningen
- **Årets væsentligste spørgsmål i forhold GDPR**
Et udpluk af de væsentligste emneområder:
 - Brug af AI produkter
 - Brug af fotos
 - Brug af sociale platforme
 - Brug af noter ved eksamen
 - Forhold vedr. samtykkeerklæring
 - Dele medarbejderoplysninger internt
 - Dele medarbejderoplysninger med fagforbund
 - Forhold vedr. brug af eksterne parter
 - Arkivering af elevdata og dokumenter
 - Slette data
 - Videregivelse af data

- Brug af podcast
- Hvidvaskloven
- Brug af spørgeskemaer
- Brug af private telefoner
- Brug af Google education

Svarene på ovenstående spørgsmål og alle øvrige relevante vil løbende blive lagt ind i vores fælles teamskanal, hvor alle i FGU, der ønsker det, kan få adgang.

Hensigten er at få akkumuleret et Q/A område i Teams, hvor alle efterfølgende kan søge svar på de væsentligste GDPR-relaterede spørgsmål, der opstår i årets løb.

Databehandleraftaler

I 2025 har der i forhold til databehandlere, ikke været nogen speciel aktivitet. Nye er kommet til og andre er ophørt.

Jeg oplever at flere og flere sender nye databehandleraftaler til gennemgang inden underskrift, hvilket jeg klart bifalder. Det er nu en gang lettere at få rettet mangelfulde databehandleraftaler inden de underskrives.

Som sædvanligt på denne tid af året er jeg i gang med gennemførelse af det årlige tilsyn med vore databehandlere, der munder ud i en individuel tilsynsrapport, som forventes at blive fremsendt og gennemgået med hver enkelt institution primo marts 2025.

Krav og pligter

Som sektor og hver institution individuelt skal vi ubetinget overholde de krav Databeskyttelsesforordningen stiller. Efterlever vi ikke dette, kan det få alvorlige konsekvenser for den enkelte institution, spændende fra dårlig omtale i lokalavisen til bødeforlæg i den kedelige kategori.

Generelt mener jeg, at FGU som helhed har godt styr på reglerne, men det betyder til gengæld ikke at vi kan slække på kravene til hinanden i forhold til, hvordan vi skal efterleve og opfylde de regler og krav der stilles til FGU fra lovgivningens side.

Grunden til at jeg igen i år understreger dette, er at vi i det daglige behandler mange følsomme data om vore elever, hvoraf mange tilhører en udsat gruppe, som vi skal passe på og værne om. Vi bliver i højere grad vandt til den teknologiske udvikling og håndtering af mange data hver dag, og derfor er det vigtigt vi fastholder fokus og ikke slækker på reglerne.

DPO'ens rolle i FGU

Som det fremgår af ovenstående, er min rolle i hverdagen af ganske stor diversitet, med GDPR som den langt overvejende hovedopgave, hvilket er helt i overensstemmelse med forordningens artikel 38, stk. 6.

I den forbindelse er det vigtigt at påpege, at min rolle, jf. forordningens artikel 39 som DPO udelukkende er rådgivende, hvorfor ledelsen på institutionerne til enhver tid kan tilsidesætte min rådgivning og beslutte, hvad de finder rigtigt, hvis de er uenige.

Med venlig hilsen

Ivan Sommer
DPO – FGU Danmark
M: iso@fgu.dk
T: 2782 7300