

Baggrund for persondatapolitikken

Gribskov Gymnasiums persondatapolitik er udarbejdet i overensstemmelse med kravene i Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (betegnet ”forordningen” i det følgende).

Persondatapolitikken gælder for alle ansatte på Gribskov Gymnasium, der behandler personoplysninger, samt for samarbejdspartnere (databehandlere), der udfører arbejde på vegne af Gribskov Gymnasium

Persondatapolitikken forventes godkendt på Gribskov Gymnasiums bestyrelsesmøde den 6. september 2018.

Formål

Formålet med persondatapolitikken er at fastlægge rammerne for behandling af personoplysninger på Gribskov Gymnasium.

Definitioner

- **Personoplysninger** er enhver form for information om en identificeret eller identificerbar fysisk person (den registrerede); ved identificerbar fysisk person forstås en fysisk person, der direkte eller indirekte kan identificeres, navnlig ved en identifikator som f.eks. et navn, et identifikationsnummer, lokaliseringsdata, eller et eller flere elementer, der er særlige for denne fysiske persons fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sociale identitet.
- **Den registrerede** er den fysiske person, som personoplysningerne vedrører, fx elever, medarbejdere, samarbejdspartnere og andre.
- **Behandling af personoplysninger** skal fortolkes bredt. Begrebet ”behandling” dækker over enhver aktivitet eller en række af aktiviteter, som personoplysninger gøres til genstand for. Det kan fx være indsamling, registrering, organisering, systematisering, opbevaring, ændring, søgning, formidling og sletning.
- **Dataansvarlig** er den person eller myndighed/organisation, der alene eller sammen med andre afgør, til hvilke formål og med hvilke hjælpemidler der må foretages behandling af personoplysninger.
- **Databehandler** er den, der behandler personoplysninger på den dataansvarliges vegne – dvs. arbejder under instruks af den dataansvarlige. Databehandler er i henhold til forordningen forpligtet til at føre fortegnelse over behandlingskategorier, der føres på vegne af den dataansvarlige.
- **Risiko for den registrerede** er risikoen for, at den registrerede bliver udsat for en fysisk, materiel eller immateriel skade, herunder tab af kontrol over sine personoplysninger,

begrænsning af sine rettigheder, forskelsbehandling, identitetstyveri, finansielle tab og sociale konsekvenser, så som skade på omdømme.

- **Databeskyttelsesrådgiveren (DPO)** er en uafhængig person med ekspertise i databeskyttelsesret og –praksis, der skal inddrages i alle spørgsmål om databeskyttelse og rådgive om de databeskyttelsesretlige regler hos Gribskov Gymnasium. Databeskyttelsesrådgiverens funktion er at overvåge, at Gribskov Gymnasium overholder reglerne i forordningen. Databeskyttelsesrådgiveren er en integreret del af Gribskov Gymnasium, og kan efter omstændighederne have andre arbejdsopgaver.
- **Brud på persondatasikkerheden** dækker over alle tilfælde, der fører til hændelig eller ulovlig tilintetgørelse, tab, eller ændring af personoplysninger såvel som uautoriseret videregivelse af eller adgang til personoplysninger.
- **Tekniske og organisatoriske sikkerhedsforanstaltninger** skal vurderes ved en risikovurdering af behandlingen af personoplysninger. Tekniske sikkerhedsforanstaltninger er blandt andet antivirusprogrammer og firewalls, som sikrer, at uvedkommende ikke kan få adgang til it-systemer med personoplysninger. Organisatoriske sikkerhedsforanstaltninger består blandt andet i, at vores medarbejdere er instrueret i og uddannet til at håndtere behandlingen af personoplysningerne korrekt og sikkert.

Ansvarsfordeling

Ledelse og medarbejdere på Gribskov Gymnasium er forpligtede til at overholde forordningens krav og regler.

Øverste ledelse (bestyrelsen)

Det er den øverste ledelse, der har det endelige ansvar for at Gribskov Gymnasium behandler personoplysninger i overensstemmelse med gældende lovgivning. Bestyrelsens rolle er at foretage dokumenterede ledelsesmæssige beslutninger i relation til beskyttelsen af personoplysninger på Gribskov Gymnasium.

Den ledelsesmæssige forankring er reguleret i databeskyttelsesforordningens artikel 5, stk. 2.

Daglig ledelse (Rektor)

Rektor er ansvarlig for, at formålene med behandling af personoplysninger er i overensstemmelse med gældende lovgivning, samt at retningslinjerne til understøttelse af politikken, er kommunikeret klart og tydeligt til medarbejderne.

Databeskyttelsesrådgiver (DPO)

DPO'ens rolle er at overvåge, at Gribskov Gymnasium overholder gældende regler for beskyttelse af personoplysninger, herunder at stå til rådighed for hele skolen i forhold til rådgivning på området. DPO'en er endvidere Gribskov Gymnasiums kontaktperson udadtil – både i forhold til de registrerede og i forhold til Datatilsynet eller andre parter. DPO'en rapporterer til det øverste ledelsesniveau.

Medarbejdere

Medarbejdere, der behandler personoplysninger, er ansvarlige for at gøre sig bekendt med formålene med behandlingen og de retningslinjer, der er relevante for udførelsen af deres arbejde.

Ansvarlighed

Når Gribskov Gymnasium behandler personoplysninger, udviser vi altid ansvarlighed. Det gøres bl.a. ved at dokumentere de beslutninger, vi træffer, de organisatoriske og tekniske foranstaltninger vi udfører, samt de retningslinjer og kontroller, vi implementerer i forbindelse med behandlingen af personoplysninger.

Medarbejdere og ledelse er ansvarlige for at gøre sig bekendte med Gribskov Gymnasiums retningslinjer om behandling af personoplysninger, der er relevante for udførelsen af arbejdet.

Lovlighed, rimelighed og gennemsigtighed

Formålet er at sætte rammerne, således at Gribskov Gymnasium behandler personoplysninger forsvarligt og i overensstemmelse med gældende lovgivning, jf. databeskyttelsesforordningens artikel 5.

Gribskov Gymnasium behandler personoplysninger i overensstemmelse med god databehandlingsskik. Det indebærer bl.a. at Gribskov Gymnasium kun behandler personoplysninger til lovlige, rimelige og legitime formål, som kan dokumenteres.

Gribskov Gymnasium indsamler, opbevarer og behandler kun personoplysninger, der er nødvendige i relation til det angivne formål. Det betyder, at vi aktivt begrænser indsamlingen og behandlingen til det nødvendige.

Gribskov Gymnasium begrænser behandlingen af personoplysninger, så behandlingen ikke er uforenelig med det oprindelige formål. Endvidere sikrer vi, at personoplysningerne ikke opbevares i et længere tidsrum end det, der er nødvendigt for at opfylde formålet med behandlingen. Når personoplysningerne ikke længere er nødvendige for det angivne formål, sikrer vi, at de enten slettes eller at der træffes andre tekniske og organisatoriske foranstaltninger, eksempelvis anonymisering, således at den registrerede ikke længere kan identificeres ud fra oplysningerne.

Såfremt Gribskov Gymnasium bliver gjort opmærksomme på at de omfattede personoplysninger er urigtige eller mangelfulde i forhold til det angivne formål, ajourfører vi oplysningerne.

Kravene for god databehandlingsskik er uddybet i ”Retningslinje om god databehandlingsskik”.

Hjemmelsgrundlag

Formålet er at sikre, at Gribskov Gymnasium behandler personoplysninger på baggrund af et fyldigt hjemmelsgrundlag, jf. databeskyttelsesforordningens kapitel 2 samt databeskyttelseslovens kapitel 3.

Gribskov Gymnasium behandler kun personoplysninger, når vi har et lovligt grundlag.

Behandling af almindelige personoplysninger sker i overensstemmelse med databeskyttelsesforordningens artikel 6.

Behandling af følsomme personoplysninger sker i overensstemmelse med reglerne i databeskyttelsesforordningens artikel 9.

Kravene til behandlingsgrundlag er uddybet i ”Retningslinje om behandlingsgrundlag”.

Overførsel til 3. lande

Formålet er at sikre, at Gribskov Gymnasium ikke overfører personoplysninger til lande uden for EU/EØS, uden der foreligger et lovligt overførselsgrundlag, jf. databeskyttelsesforordningens kapitel 5.

Gribskov Gymnasium overfører kun personoplysninger til lande uden for EU/EØS i de tilfælde, hvor vi har et lovligt overførselsgrundlag.

Ansatte på Gribskov Gymnasium, kan til enhver tid søge rådgivning om overførselsgrundlag hos skolens databeskyttelsesrådgiver.

Kravene til overførsel af personoplysninger til tredjelande er uddybet i ”Retningslinje om overførsel til 3. lande”.

Fortegnelser over behandlingsaktiviteter

Formålet er at sikre, at Gribskov Gymnasium fører de lovpligtige fortegnelser over behandlingsaktiviteter, som efter anmodning skal stilles til rådighed for Datatilsynet, jf. databeskyttelsesforordningens artikel 30.

Fortegnelserne kan ligeledes anvendes som hjælp til at sikre, at der foreligger et grundlag for vurdering af risici for behandling af personoplysninger.

Gribskov Gymnasium fører en fortegnelse over de behandlinger af personoplysninger, vi foretager, og sørger aktivt for at holde fortegnelsen opdateret.

Gribskov Gymnasiums medarbejdere, er forpligtede til at underrette den procesansvarlige om ændringer og lignende i forhold til den måde, hvorpå personoplysninger behandles.

Kravene til fortegnelsen er uddybet i ”Retningslinje om fortegnelse over behandlingsaktiviteter”.

Den registreredes rettigheder

Formålet er at sikre, at behandlingen af personoplysninger tage hensyn til den registreredes ret til at kontrollere omfanget af behandling af dennes personoplysninger, jf. databeskyttelsesforordningens kapitel 3.

Når Gribskov Gymnasium behandler personoplysninger overholder vi vores oplysningspligt, således behandlingen sker på en åben og oplyst måde, samt at den registrerede kender sine rettigheder.

Gribskov Gymnasium bistår den registrerede med at udøve sine rettigheder, herunder:

- Indsigt i de behandlinger af personoplysninger, [indsæt skole] foretager om denne
- Berigtigelse, såfremt personoplysningerne er forkerte eller mangelfulde
- Sletning af de personoplysninger vi behandler
- Begrænsning af behandlingen af personoplysninger
- Dataportabilitet

- Behandling af indsigelse mod behandling af personoplysninger

Kravene til opfyldelse af den registreredes rettigheder er uddybet i ”Retningslinje om den registreredes rettigheder”.

Dataansvarlig og databehandler

Formålet er at sikre, at det er afklaret hvorvidt Gribskov Gymnasium agerer som dataansvarlig eller som databehandler, jf. databeskyttelsesforordningens kapitel 4.

Endvidere er formålet at anskueliggøre hvilke databehandlere Gribskov Gymnasium benytter, samt at sikre at der er indgået databehandleraftale med disse.

Når Gribskov Gymnasium er dataansvarlig, sikrer vi, at eventuelle databehandlere kan leve op til forordningens krav, og stille de fornødne garantier for behandling af personoplysninger på vegne af Gribskov Gymnasium.

Gribskov Gymnasium sikrer, at databehandleren er instrueret i, hvordan denne skal behandle de personoplysninger, som Gribskov Gymnasium er dataansvarlige for. Endvidere sikrer vi, at der er indgået databehandleraftaler med alle databehandlere.

Når Gribskov Gymnasium er databehandler på vegne af en anden dataansvarlig, sikrer vi, at vi udelukkende behandler personoplysninger på baggrund af den dataansvarliges instruks. Vi sørger endvidere for, at Gribskov Gymnasium ikke benytter sig af underdatabehandlere, der ikke er godkendt af den dataansvarlige.

Risikovurdering

Formålet er at sikre, at eventuelle risici for den registrerede identificeres forud for behandlingen af dennes personoplysninger.

Gribskov Gymnasium foretager altid en risikovurdering i forbindelse med behandling af personoplysninger. Risikovurderingen tager udgangspunkt i behandlingens karakter, omfang, sammenhæng og formål samt de anvendte systemer.

Risikovurdering er baseret på en konsekvensvurdering for den registrerede samt en sandsynlighedsvurdering for at konsekvensen indtræffer.

Risikovurderingerne dokumenteres og godkendes af den daglige ledelse.

Kravene til risikovurderingerne er uddybet i ”Retningslinje om risikovurderinger”.

Konsekvensanalyser (DPIA)

Formålet er at sikre, at Gribskov Gymnasium udarbejder en konsekvensanalyse (DPIA) forud for behandling af personoplysninger, der sandsynligvis indebærer en høj risiko for den registrerede, jf. databeskyttelsesforordningens kapitel 4 afdeling 2.

Hvis det vurderes i den almindelige risikovurdering, at en behandling af personoplysninger sandsynligvis vil indebære høj risiko for den registreredes rettigheder, udfører Gribskov Gymnasium

en konsekvensanalyse. Konsekvensanalysen skal hjælpe med at fastlægge de foranstaltninger, vi påtænker, kan imødekomme disse risici.

Behandlingssikkerhed

Formålet er at sikre, at Gribskov Gymnasium med udgangspunkt i en risikovurdering, yder tilstrækkelig sikkerhed ved behandling af personoplysninger, jf. databeskyttelsesforordningens kapitel 4 afdeling 2.

På baggrund af den udarbejdede risikovurdering og eventuelle konsekvensanalyse fastlægges hvilke sikkerhedsforanstaltninger, der skal implementeres, således det sikres, at der er et tilstrækkeligt sikkerhedsniveau, når Gribskov Gymnasium behandler personoplysninger.

De fastlagte sikkerhedsforanstaltninger revurderes løbende.

Gribskov Gymnasium sikrer ligeledes at it-løsninger, der anvendes til behandling af personoplysninger, er designet hertil.

Kravene til behandlingssikkerhed er uddybet i ”Retningslinje om behandlingssikkerhed”.

Brud på persondatasikkerheden

Formålet er at sikre, at brud på persondatasikkerheden håndteres korrekt, jf. databeskyttelsesforordningens artikel 33 og 34.

I det tilfælde, at der sker brud på persondatasikkerheden, anmelder Gribskov Gymnasium bruddet til Datatilsynet uden unødigt forsinkelse, og senest 72 timer efter, bruddet er blevet opdaget, medmindre det er usandsynligt at bruddet indebærer en risiko for den registrerede.

Hvis bruddet sandsynligvis indebærer en høj risiko for den registrerede, underretter Gribskov Gymnasium den registrerede om bruddet.

Kravene til håndtering af brud på persondatasikkerheden er uddybet i ”Retningslinje om brud på persondatasikkerheden”.

Databeskyttelsesrådgiver

Formålet er at sikre, at Gribskov Gymnasiums databeskyttelsesrådgivers rolle, herunder stillingsbeskrivelse og opgaver er i overensstemmelse med databeskyttelsesforordningens krav, jf. artikel 37.

Gribskov Gymnasiums databeskyttelsesrådgiver er udvalgt på baggrund af sine faglige kvalifikationer, herunder ekspertise inden for databeskyttelsesret.

Databeskyttelsesrådgiverens rolle er at overvåge, at Gribskov Gymnasium overholder gældende regler på området, herunder at stå til rådighed for hele skolen i forhold til rådgivning på området. Databeskyttelsesrådgiveren er endvidere Gribskov Gymnasiums kontaktperson udadtil – både i forhold til de registrerede og i forhold til Datatilsynet eller andre.

Ansatte på Gribskov Gymnasium, der er i tvivl om indholdet i denne persondatapolitik eller de tilhørende retningslinjerne, kan til enhver tid kontakte databeskyttelsesrådgiveren.

Kontaktoplysninger til Gribskov Gymnasium s databeskyttelsesrådgiver:

Anne Schultz

ansc@itcfyn.dk / 5138 3253

Databeskyttelsesrådgiverens rolle, opgaver og ansvar er uddybet i ”Retningslinje for databeskyttelsesrådgivere”.

Datatilsynet

Formålet er at sikre, at henvendelser fra Datatilsynet omkring tilsyn og andre forespørgsler håndteres korrekt, herunder at Datatilsynet modtager den relevante dokumentation, jf. databeskyttelsesforordningens kapitel 6.

Gribskov Gymnasiums databeskyttelsesrådgiver bistår Datatilsynet i forbindelse med tilsynssager og andre forespørgsler.

Kontrol og dokumentation

Bestyrelsen på Gribskov Gymnasium sikrer, at overholdelsen af denne persondatapolitik er dokumenteret, og at dokumentationen løbende opdateres.

Dokumentejer, godkender og versionering

Ejer: Hanne B. Nielsen

Godkender: Thomas Krumholt, uddannelsesleder

Dato	Version	Forfatter	Ændringsbeskrivelse
25.5.2018	1.0	HBN	-