GAMMEL
HELLERUP
GYMNASIUM

Persondatapolitik for Gammel Hellerup Gymnasium

Indhold

Baggrund for persondatapolitikken 1
Formål 2
Definitioner 2
Ansvarsfordeling 3
Ansvarlighed 3
Lovlighed, rimelighed og gennemsigtighed 4
Hjemmelsgrundlag 4
Overførsel til 3. lande 5
Fortegnelser over behandlingsaktiviteter 5
Den registreredes rettigheder 5
Dataansvarlig og databehandler 6
Risikovurdering 6
Konsekvensanalyser (DPIA) 7
Behandlingssikkerhed 7
Brud på persondatasikkerheden 7
Databeskyttelsesrådgiver 8
Datatilsynet 8
Kontrol og dokumentation 8
Dokumentejer, godkender og versionering 9

Baggrund for persondatapolitikken

Denne 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 Gammel Hellerup Gymnasium, der behandler personoplysninger, samt for samarbejdspartnere (databehandlere), der udfører arbejde på vegne af Gammel Hellerup Gymnasium.

Formål

Formålet med persondatapolitikken er at fastlægge rammerne for behandling af personoplysninger på Gammel Hellerup 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 kunder, medarbejdere, leverandører, 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 Gammel Hellerup Gymnasium. Databeskyttelsesrådgiverens funktion er at understøtte, at Gammel Hellerup Gymnasium overholder reglerne i forordningen. Databeskyttelsesrådgiveren er en integreret del af Gammel Hellerup 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 er forpligtet til at overholde forordningens krav og regler.

Øverste ledelse (bestyrelsen)
Det er den øverste ledelse, der har det endelige ansvar for at Gammel Hellerup Gymnasium behandler personoplysninger i overensstemmelse med gældende lovgivning. Bestyrelsens rolle er at foretage dokumenterede ledelsesmæssige beslutninger i relation til beskyttelsen af personoplysninger på Gammel Hellerup 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 kontrollere, at Gammel Hellerup 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 Gammel Hellerup 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 Gammel Hellerup 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 Gammel Hellerup Gymnasiums retningslinjer om behandling af personoplysninger, der er relevante for udførslen af arbejdet.

Lovlighed, rimelighed og gennemsigtighed

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

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

Gammel Hellerup 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.

Gammel Hellerup Gymnasium begrænser behandlingen af personoplysninger, så behandlingen ikke er uforenelig med det oprindelig 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 Gammel Hellerup Gymnasium bliver gjort opmærksom 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 Gammel Hellerup Gymnasium behandler personoplysninger på baggrund af et fyldigt hjemmelsgrundlag, jf. databeskyttelsesforordningens kapitel 2 samt databeskyttelses-lovens kapitel 3.

Gammel Hellerup 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 Gammel Hellerup Gymnasium ikke overfører personoplysninger til lande uden for EU/EØS, uden der foreligger et lovligt overførselsgrundlag, jf. databeskyttelses-forordningens kapitel 5.

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

Fortegnelser over behandlingsaktiviteter

Formålet er at sikre, at Gammel Hellerup 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.

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

Gammel Hellerup 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 tager hensyn til den registreredes ret til at kontrollere omfanget af behandling af dennes personoplysninger, jf. databeskyttelsesforordningens kapitel 3.

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

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

- Indsigt i de behandlinger af personoplysninger, Gammel Hellerup Gymnasium 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 Gammel Hellerup Gymnasium agerer som dataansvarlig eller som databehandler, jf. databeskyttelsesforordningens kapitel 4. Endvidere er formålet at anskueliggøre, hvilke databehandlere Gammel Hellerup Gymnasium benytter, samt at sikre at der er indgået databehandleraftale med disse.

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

Når Gammel Hellerup 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 Gammel Hellerup 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.

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

Behandlingssikkerhed

Formålet er at sikre, at Gammel Hellerup 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 at det sikres, at der er et tilstrækkeligt sikkerhedsniveau, når Gammel Hellerup Gymnasium behandler personoplysninger.

De fastlagte sikkerhedsforanstaltninger revurderes løbende.

Gammel Hellerup 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 Gammel Hellerup Gymnasium bruddet til Datatilsynet uden unødig forsinkelse, og senest 72 timer efter, at 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 Gammel Hellerup 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 Gammel Hellerup Gymnasiums databeskyttelsesrådgivers rolle, herunder stillingsbeskrivelse og opgaver er i overensstemmelse med databeskyttelsesforordningens krav, jf. artikel 37.

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

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

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

Kontaktoplysninger til Gammel Hellerup Gymnasiums databeskyttelsesrådgiver:

Navn: Jacob Naur
E-mail: jgn@hejm.dk
Telefonnummer: 61440706

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.

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

Se endvidere "Retningslinje for databeskyttelsesrådgivere".

Kontrol og dokumentation

Bestyrelsen på Gammel Hellerup Gymnasium sikrer, at overholdelsen af denne persondata-politik er dokumenteret, og at dokumentationen løbende opdateres.

Dokumentejer, godkender og versionering

Ejer: Jesper Mathorne Jacobsen
Godkender: Stig Wall-Gremstrup (Bestyrelsesformand)

Dato	Version	Forfatter	Ændringsbeskrivelse
21.03.2018	1.0	JJ	-

6/4-18 _____

Dato Stig Wall-Gremstrup (Bestyrelsesformand)