Retningslinje om ansvarsfordeling - dataansvarlig vs. databehandler

Anvendelsesområde

Retningslinje om ansvarsfordeling 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) og gælder for alle ansatte på Gefion Gymnasium, der behandler personoplysninger.

Formål

Formålet med denne retningslinje er at sikre, at Gefion Gymnasium altid er bevidst om i hvilke tilfælde, vi er dataansvarlige og i hvilke tilfælde vi er databehandlere i relation til en konkret behandling af personoplysninger.
Derudover skal retningslinjen sikre, at vi stiller de rigtige krav til vores databehandlere, samt at vi selv overholder de krav, som vi er pålagt, når vi databehandlere.

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 medarbejdere, elever, 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.

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 Gefion Gymnasium. Databeskyttelsesrådgiverens funktion er at understøtte, at den Gefion Gymnasium overholder reglerne i forordningen. Databeskyttelsesrådgiveren er en integreret del af Gefion Gymnasium, og kan efter omstændighederne have andre arbejdsopgaver.

Ansvarsfordelingen

Den dataansvarlige er forordningens centrale aktør, og det er den dataansvarlige, der er ansvarlige for at behandlingen af personoplysninger er i overensstemmelse med forordningens krav og regler.

Databehandleren er som udgangspunkt den dataansvarliges underordnede, og skal således handle efter dennes instruks, men på grund af den stigende teknologiske udvikling har databehandleren fået en mere fremtræden rolle.

Rollefordelingen mellem de to parter skal være klar, således der skabes størst mulig tryghed hos den registrerede.

Det er vigtigt at bemærke, at Gefion Gymnasium kan have forskellige roller afhængigt af den pågældende databehandling. Ved nogle databehandlinger kan vi således være dataansvarlige, mens vi ved andre databehandlinger kan være databehandlere på vegne af en anden dataansvarlig.

Ved vurderingen af hvilken rolle Gefion Gymnasium har i forbindelse med en konkret databehandling, kan vi tage udgangspunkt i følgende:

- Hvem bestemmer formålet med databehandlingen?
- Hvem udfører vi databehandlingen for?
- Hvem beslutter hvilke hjælpemidler vi skal anvende i forbindelse med databehandlingen?

Dataansvarlig

Hvis Gefion Gymnasium har bestemt formålet med databehandlingen samt besluttet hvilke hjælpemidler, vi skal benytte hertil, er vi dataansvarlig myndighed.

Det er vigtigt at bemærke, at det er Gefion Gymnasium, der er dataansvarlig, og altså ikke den enkelte ansatte.

Når Gefion Gymnasium er dataansvarlig, er vi ikke blot forpligtet til at overholde forordningens regler, men vi også forpligtet til at påvise overholdelsen.

Dataansvarliges forpligtelser

Gefion Gymnasium skal ud fra en vurdering af den konkrete databehandlings karakter, formål, omfang og hermed forbundne sandsynlige risici gennemføre tekniske og organisatoriske foranstaltninger for at sikre, at behandlingen sker i overensstemmelse med forordningens bestemmelser.

Vi skal med andre ord foretage en risikovurdering for hver databehandling for at vurdere, hvilke foranstaltninger vi skal gennemføre ved den konkrete databehandling. Dette gælder ligeledes, hvis databehandlingen ændrer karakter og/eller omfang.

Dataansvarliges brug af databehandlere

Når Gefion Gymnasium som dataansvarlig anvender databehandlere til en konkret databehandling, skal vi sikre os, at vi udelukkende anvender databehandlere, som er i stande til at overholde forordningens krav, herunder at databehandleren i samarbejde med Gefion Gymnasium kan sikre overholdelsen af de registreredes rettigheder.

Derudover skal vi sikre os, at vi altid indgår en databehandleraftale med databehandleren. Databehandleraftalen fastlægger rammerne for den konkrete databehandling, og samtidig indeholder aftalen også en instruks, hvori Gefion Gymnasium har beskrevet vores krav til databehandlingen, som databehandleren skal efterleve.

I tilfælde af at vores databehandlere ønsker at benytte underdatabehandlere skal vi sikre os, at vores databehandlere enten

- Modtager vores *forudgående specifikke skriftlige samtykke* hertil, eller
- Har fået en *forudgående generel skriftlig godkendelse* til at benytte underdatabehandlere

En generel skriftlig godkendelse er en godkendelse til at databehandleren kan tilføje eller erstatte en underdatabehandler uden at spørge Gefion Gymnasium. Vi skal sikre os, at databehandleren instrueres i, at denne altid skal underrette Gefion Gymnasium om eventuelle ændringer i brugen af underdatabehandlere, eksempelvis hvis databehandleren tilføjer eller fjerner en underdatabehandler.

I den forbindelse skal vi ligeledes instruere vores databehandlere i at indgå en databehandleraftale med underdatabehandlere, som er i overensstemmelse med den databehandleraftale Gefion Gymnasium har med vores databehandler.

Databehandler

Hvis Gefion Gymnasium ikke selv har bestemt formålet med databehandlingen, og vi i stedet handler på vegne af en anden dataansvarlig, er vi som udgangspunkt databehandlere for den dataansvarlige.

Når vi er databehandlere, handler vi således udelukkende efter instruks fra den dataansvarlige.

Databehandlerens forpligtelser

Når Gefion Gymnasium er databehandler skal vi sikre, at vi har et overblik over de databehandleraftaler, som vi har indgået med de dataansvarlige.

Databehandleren skal sikre, at der føres den fornødne fortegnelse over behandlingsaktiviteter, som udføres på vegne af den dataansvarlige. Se *retningslinje om fortegnelse*.

Endvidere skal det sikres, at databehandleren overholder de krav, som fremgår af databehandleraftalen, se nedenfor.

Fælles dataansvarlige

I visse tilfælde kan Gefion Gymnasium være fælles dataansvarlige med en anden dataansvarlig myndighed. Dette indebærer, at vi i fællesskab skal fastlægge ansvarsfordelingen i forhold til overholdelsen af forordningens regler, herunder i særdeleshed håndteringen af de registreredes rettigheder.

Hvis Gefion Gymnasium er fælles dataansvarlig med en anden myndighed, sikrer vi os, at vi fortsat overholder de krav, der er til den dataansvarlige, herunder bl.a. forpligtelsen til at føre en fortegnelse over behandlingsaktiviteter.

Krav til databehandleraftalen

Databehandleraftalen indgås som et retligt dokument mellem dataansvarlig og databehandler. Aftalen fastsætter formålet og varigheden med databehandlingen, herunder databehandlingens omfang, hvilke typer personoplysninger, der er tale om, og hvilke kategorier af registrerede personer, behandlingen omfatter.

Databehandleraftalen skal således indeholde:

- Beskrivelse af parterne; dataansvarlig og databehandlere, herunder underdatabehandlere
- Beskrivelse af formålet med databehandlingen
- Beskrivelse af kategorier af registrerede
- Beskrivelse af de typer af personoplysninger, der behandles, eksempelvis "helbredsoplysninger", "kontaktoplysninger".

- Beskrivelse af dataansvarliges forpligtelser og rettigheder i henhold til databeskyttelsesforordningen
- En instruks til databehandleren om hvordan denne skal behandle personoplysninger på vegne af dataansvarlige
- Beskrivelse af de sikkerhedsforanstaltninger, som databehandleren har iværksat
- Beskrivelse af i hvilket omfang databehandleren anvender underdatabehandlere
- Beskrivelse af databehandlerens sletning og/eller tilbagelevering af personoplysninger
- Beskrivelse af databehandlerens bistand til den dataansvarlige i forbindelse med bl.a. sikkerhedsbrud, håndtering af de registreredes rettigheder og ophør af databehandling

Se endvidere Gefion Gymnasiums databehandleraftaleskabelon.

Kontrol og dokumentation

Gefion Gymnasium skal sikre, at der løbende foretages en dokumenteret kontrol af, at denne retningslinje efterleves. Kontrollen godkendes af bestyrelsen for Gefion Gymnasium.

Gefion Gymnasium dokumenterer

- At vi har et overblik over de databehandlinger hvor vi henholdsvis er dataansvarlige og databehandlere
- At vi har indgået de fornødne databehandleraftaler – såvel som dataansvarlige som databehandlere
- At den løbende kontrol er udført

Dokumentejer, godkender og versionering

Ejer: Bettina Poulsen

Godkender: Andreas Møller Lange

Dato	Version	Forfatter	Ændringsbeskrivelse
5. april	1.0	JUS	-
30. maj 2018	2.0	MSI	Tilrettet med Gefion Gymnasiums oplysninger