Bilag 3

Retningslinje om behandlingsgrundlag

Anvendelsesområde

Retningslinje om overførsel til tredjelande 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 Ringkjøbing Gymnasium, der behandler personoplysninger samt for samarbejdspartnere (databehandlere), der udfører opgaver på vegne af Ringkjøbing Gymnasium.

Formål

Formålet med denne retningslinje er at sikre, at Ringkjøbing Gymnasium foruden de almindelige behandlingsregler ligeledes iagttager databeskyttelsesforordningens regler omkring overførsel af personoplysninger til tredjelande, jf. databeskyttelsesforordningens kapitel V.

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 fx 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, kursister, 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.

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.

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 på Ringkjøbing Gymnasium. Databeskyttelsesrådgiverens funktion er at understøtte, at Ringkjøbing Gymnasium overholder reglerne i forordningen. Databeskyttelsesrådgiveren er ansat på Ringkjøbing Gymnasium.

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.

Hvad er et tredjeland?

Et tredjeland er et land, som hverken er medlem af EU eller EØS[1]. I databeskyttelsesforordningen skelnes endvidere mellem sikre tredjelande og usikre tredjelande.
At være et sikkert tredjeland betyder, at EU-Kommissionen har taget stilling til landets sikkerhedsniveau.
Uanset om der er tale om en overførsel til et sikkert eller et usikkert tredjeland, skal det modtagende land altid leve op til de fire essentielle europæiske værdier:

1. Myndigheder i tredjelandes adgang til og brug af personoplysninger hidrørende fra EU skal ske på grundlag af klare, præcise og tilgængelige regler.

2. Myndigheder i tredjelandes adgang til og brug af personoplysninger hidrørende fra EU skal være nødvendig og proportional (der skal være balance mellem formålet (national sikkerhed) og indgrebet i de registreredes ret til beskyttelse af deres privatliv).

3. Der skal være en uafhængig og effektiv tilsynsmyndighed i tredjelandet.

4. Der skal være tilgængelige og effektive retsmidler for de registrerede i tredjelandet. Konsekvensen af de fire essentielle europæiske garantier er, at Ringkjøbing Gymnasium ikke kan overføre personoplysninger til et tredjeland, hvis dette tredjelands lovgivning, praksisser m.v. ikke muliggør en efterlevelse af garantierne.

Hvad er en overførsel?

Begrebet ”overførsel” dækker både over den situation, hvor Ringkjøbing Gymnasium **videregiver** personoplysninger til en ny dataansvarlig i et tredjeland og den situation, hvor Ringkjøbing Gymnasium **overlader** en behandling af personoplysninger til en databehandler i tredjeland.
En overførsel kan fx bestå i en elektronisk transmission eller i en fremsendelse af en USB-nøgle, men en overførsel kan også bestå i, at personer i et tredjeland gives ”kigge-adgang” til oplysninger, der befinder sig i EU.

Eksempel:
Ringkjøbing Gymnasium benytter en virksomhed i Indien til it-support. De indiske medarbejdere har ikke-teknisk adgang til at lagre eller printe personoplysninger, men har alene adgang til at se oplysningerne.

[1] https://www.eu.dk/faq/alle-faqs/hvad-er-efta-og-eoes

I dette tilfælde vil der være tale om en overførsel til et (usikkert) tredjeland, da personoplysninger i Danmark gøres tilgængelige for medarbejderne i den indiske virksomhed. Det gør ingen forskel, at oplysningerne alene kan ses i Indien eller, at medarbejderne ikke forstår dansk.

OBS! Det bemærkes, at foruden et gyldigt overførselsgrundlag er Ringkjøbing Gymnasium forpligtet til at indgå de fornødne databehandleraftaler, såfremt overførslen af personoplysninger sker til en databehandler.

I ovenstående eksempel vil der således foruden et gyldigt overførselsgrundlag ligeledes skulle indgås en databehandleraftale mellem Ringkjøbing Gymnasium og den indiske it-support.

Overførsel til sikre tredjelande?

Når Kommissionen har truffet afgørelse om, at et tredjeland er sikkert, betyder det, at der kan overføres personoplysninger til en modtager i det pågældende land, uden at der først skal søges om godkendelse fra Datatilsynet. Dette er dog under forudsætning af, at databeskyttelsesforordningens øvrige regler samt de fire essentielle europæiske garantier overholdes.
På nuværende tidspunkt har Kommissionen vurderet, at følgende lande yder et tilstrækkeligt sikkerhedsniveau:

- Andorra
- Argentina
- Færøerne
- Guernsey
- Isle of Man
- Israel
- Jersey
- New Zealand
- Schweiz
- Uruguay

En opdateret liste kan findes på Kommissionens hjemmeside[2].
Kommissionen har som tillæg til ovenstående vurderet, at overførsler til amerikanske virksomheder, der har tilsluttet sig den såkaldte *Privacy Shield*, kan betragtes som overførsler til et sikkert tredjeland.

Overførsel til usikre tredjelande – fornødne garantier?

I de situationer hvor Ringkjøbing Gymnasium ønsker at overføre personoplysninger til et usikkert tredjeland, skal vi give de fornødne garantier for databeskyttelse. En fornøden garanti kan fx gives ved indgåelse af en kontrakt mellem Ringkjøbing Gymnasium og dataimportøren (enten dataansvarlig eller databehandler i tredjelandet). Nedenfor ses de muligheder, som Ringkjøbing Gymnasium har for at give de fornødne garantier:

1. Retligt bindende instrumenter (aftaler m.v.) mellem offentlige myndigheder eller organer
2. Bindende virksomhedsregler
3. Adfærdskodeks og certificeringsmekanismer
4. Standardbestemmelser om databeskyttelse
5. Ad hoc-kontrakter

Denne retningslinje gennemgår punkt 3 og 4.

[2] https://informationssikkerhed.ku.dk/english/protection-of-information-privacy/privacy-policy/the-european-commissions-decision/Decision_on_standard_contractual_clauses_-_English.pdf

Ad. 3. Adfærdskodeks og certificeringsmekanismer:
Ringkjøbing Gymnasium har mulighed for at benytte sig af adfærdskodekser og andre certificeringsmekanismer.
Adfærdskodekser og certificeringsordninger kan fungere som redskaber for dataansvarlige og databehandlere med henblik på at dokumentere, at de overholder de forpligtelser, som de er pålagt i henhold til databeskyttelsesforordningen vedrørende deres databehandlingsaktiviteter.

Certificering vil bl.a. kunne anvendes som et element i dokumentationen for, at databeskyttelsesforordningens generelle krav om *privacy by design* og *privacy by default* overholdes. Dette kan fx opnås ved at få certificeret, at de it-løsninger Ringkjøbing Gymnasium bruger, overholder kravene i databeskyttelsesforordningen.

Hvis en dataansvarlig eller en databehandler i et tredjeland tilslutter sig et godkendt adfærdskodeks eller en godkendt certificeringsordning, vil Ringkjøbing Gymnasium kunne overføre personoplysninger til den tilsluttede virksomhed uden forudgående godkendelse fra en tilsynsmyndighed.
Forskellen på adfærdskodeks og certificering ses nedenfor:

	Adfærdskodeks	**Certificering**
Formål	Opnå compliance og signalere compliance til omverdenen	Opnå compliance og signalere compliance til omverdenen
Beskrivelse	Retningslinjer for opfyldelse af forordningens krav til forskellige former for behandling af personoplysninger inden for en bestemt sektor/branche	Kontrol af at den dataansvarliges eller databehandlerens behandling af personoplysninger sker i henhold til foruddefinerede kriterier
Udstedelse	Udarbejdes af organisationer og brancheforeninger, der repræsenterer dataansvarlige eller databehandlere	Udarbejdes af akkrediterede certificeringsorganer eller kompetente tilsynsmyndigheder
Godkendelse	Godkendelse foretages af myndighederne. Et adfærdskodeks, der alene vedrører behandlingsaktiviteter i én medlemsstat, skal godkendes af den lokale tilsynsmyndighed.	Kriterierne for certificering skal godkendes af myndighederne.
Gyldighed	Ingen restriktioner	Kan udstedes for en periode på højest 3 år. Certificering kan fornyes efter udløb, hvis kriterierne fortsat overholdes.
Offentliggørelse	Tilsynsmyndigheden registrerer og offentliggør adfærdskodekserne.	Databeskyttelsesrådet samler dem i et register og gør dem offentligt tilgængelige. Databeskyttelsesrådet samler certificeringsordninger i et register og gør dem offentligt tilgængelige.

Følgende betingelser skal være opfyldt for, at et adfærdskodeks eller en certificeringsordning kan benyttes i forbindelse med overførsel af personoplysninger til at tredjeland:

- Adfærdskodekset eller certificeringsordningen skal være godkendt af den kompetente tilsynsmyndighed eller af et certificeringsorgan.
- Adfærdskodekset eller certificeringsordningen skal indeholde specifikke regler om tredjelandsoverførsel.

- Der skal foreligge et bindende tilsagn fra dataimportøren (dataansvarlig/databehandler) i et tredjeland om at anvende adfærdskodekset eller certificeringsordningens regler om tredjelandsoverførsel.
- Det bindende tilsagn skal kunne håndhæves af et kompetent kontrolorgan.

Se endvidere databeskyttelsesforordningens artikel 40-43.

Ad. 4. Standardbestemmelser om databeskyttelse:
Kommissionen har vedtaget tre typer af standardbestemmelser om databeskyttelse, der kan anvendes i forbindelse med overførsel af personoplysninger til usikre tredjelande. Standardbestemmelserne er vedtaget på baggrund af databeskyttelsesdirektivet, men de kan fortsat anvendes.

Inden Ringkjøbing Gymnasium gør brug af standardbestemmelserne, skal vi gøre os det klart, om vi overfører oplysninger til en dataansvarlig i et tredjeland eller til en databehandler i et tredjeland. Dette skyldes, at der findes forskellige standardbestemmelser til de to situationer.

De gældende standardbestemmelser for overførsel til databehandler i tredjeland og overførsel til dataansvarlig i tredjeland, kan findes på Kommissionens hjemmeside:
https://informationssikkerhed.ku.dk/english/protection-of-information-privacy/privacy-policy/the-european-commissions-decision/Decision_on_standard_contractual_clauses_-_English.pdf

Såfremt der er tale om en overladelse fra en dataansvarlig til en databehandler, skal standardkontrakten således indgås mellem dataansvarlig og databehandler. Hvis databehandler gør brug af en underdatabehandler, er Ringkjøbing Gymnasium som dataansvarlig forpligtet til at indgå en standardkontrakt direkte med underdatabehandleren.[3]

Hvis Ringkjøbing Gymnasium benytter sig af standardbestemmelserne, skal vi som udgangspunkt ikke have en specifik godkendelse fra tilsynsmyndigheden.

Det er dog vigtigt at bemærke, at der udelukkende må ændres i tekstens "*tillæg 1 og 2*". Der henvises til EU-kommissionens standardskabelon for overførsel til databehandlere i tredjeland:
https://eurlex.europa.eu/legal-content/DA-EN/TXT/?uri=CELEX:32010D0087&from=en

Hvis der yderligere ændres i teksten i standardbestemmelserne kræver dette, at Datatilsynet godkender aftalen på ny, og der er således ikke længere tale om standardbestemmelser.

Kontrol og dokumentation

Ringkjøbing Gymnasium skal sikre, at vi løbende foretager en dokumenteret kontrol af, at denne retningslinje overholdes. Kontrollen skal godkendes af Ringkjøbing Gymnasiums bestyrelse.

Ringkjøbing Gymnasium dokumenterer, at vi:

- har et overblik over vores overførsler til tredjelande
- har de fornødne overførselsgrundlag
- foruden et overførselsgrundlag indgår databehandleraftaler med vores evt. databehandlere i tredjelande

[3] Dette gør sig udelukkende gældende i forbindelse med første led af underdatabehandlere. Såfremt underdatabehandleren gør brug af en underunderdatabehandler, er den dataansvarlig kun forpligtet til at indgå en standardkontrakt med underdatabehandleren. Underdatabehandleren skal herefter indgå en databehandleraftale med under-underdatabehandleren, som pålægger denne de samme forpligtelser som dem, der påhviler underdatabehandleren, jf. Standardbestemmelse 11.