Vejen Business Colleges

Persondatapolitik

[GDPR]

Senest revideret den 9. maj 2021

Indholdsfortegnelse

Vejen Business Colleges persondatapolitik	side 3
Bilag 1: Retningslinje om god databehandlingsskik	side 10
Bilag 2: Retningslinje om behandlingsgrundlag	side 12
Bilag 3: Retningslinje om overførsel til tredjelande	side 17
Bilag 4: Retningslinje om fortegnelser over behandlingsaktiviteter	side 24
Bilag 5: Retningslinje om de registreredes rettigheder	side 29
Bilag 6: Retningslinje om risikovurderinger	side 39
Bilag 7: Retningslinje om behandlingssikkerhed	side 42
Bilag 8: Retningslinje om brud på persondatasikkerheden	side 47
Bilag 9: Retningslinje om databeskyttelsesrådgivere	side 54
Bilag 10: Retningslinje om ansvarsfordeling (dataansvarlig/ databehandler)	side 59

Vejen Business Colleges persondatapolitik

Vejen Business Colleges (VBC) 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 VBC, der behandler personoplysninger, samt for samarbejdspartnere (databehandlere), der udfører arbejde på vegne af VBC.

Persondatapolitikken er godkendt på VBC´s bestyrelsesmøde den XX. XX 2021.

Formål

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

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 VBC. Databeskyttelsesrådgiverens funktion er at overvåge, at VBC overholder reglerne i forordningen.

- **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 VBC er forpligtede til at overholde forordningens krav og regler.

Øverste ledelse (bestyrelsen)

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

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

Daglig ledelse (Forstander)

Forstander 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 VBC 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 VBCs 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 VBC 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.

Ledelsen er ansvarlig for at gøre medarbejderne bekendte med VBC´s retningslinjer om behandling af personoplysninger, der er relevante for udførslen af arbejdet.

Lovlighed, rimelighed og gennemsigtighed

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

VBC behandler personoplysninger i overensstemmelse med god databehandlingsskik.

Det indebærer bl.a. at VBC kun behandler personoplysninger til lovlige, rimelige og legitime formål, som kan dokumenteres.

VBC 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.

VBC 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 VBC 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 bilag 1 ”Retningslinje om god databehandlingsskik”.

Hjemmelsgrundlag

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

VBC 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 bilag 2 ”Retningslinje om behandlingsgrundlag”.

Overførsel til 3. lande

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

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

Ansatte på VBC, kan til enhver tid søge rådgivning om overførselsgrundlag hos skolens databeskyttelses-rådgiver.

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

Fortegnelser over behandlingsaktiviteter

Formålet er at sikre, at VBC 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.

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

VBCs 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 bilag 4 ”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 VBC behandler personoplysninger overholder vi vores oplysningspligt, således behandlingen sker på en åben og oplyst måde, samt at den registrerede kender sine rettigheder.

VBC bistår den registrerede med at udøve sine rettigheder, herunder:

- Indsigt i de behandlinger af personoplysninger, VBC 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 bilag 5 ”Retningslinje om den registreredes rettigheder”.

Dataansvarlig og databehandler

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

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

Når VBC 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 VBC.

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

Når VBC 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 VBC 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.

VBC 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 bilag 6 ”Retningslinje om risikovurderinger”.

Konsekvensanalyser (DPIA)

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

Behandlingssikkerhed

Formålet er at sikre, at VBC 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 VBC behandler personoplysninger.

De fastlagte sikkerhedsforanstaltninger revurderes løbende.

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

Kravene til behandlingssikkerhed er uddybet i bilag 7 ”Retningslinje om behandlingssikkerhed”.

Brud på persondatasikkerheden

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

I det tilfælde, at der sker brud på persondatasikkerheden, anmelder VBC bruddet til Datatilsynet uden unødig 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 VBC den registrerede om bruddet.

Kravene til håndtering af brud på persondatasikkerheden er uddybet i bilag 8 ”Retningslinje om brud på persondatasikkerheden”.

Databeskyttelsesrådgiver

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

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

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

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

Kontaktoplysninger til VBCs databeskyttelsesrådgiver:

Databeskyttelsesrådgiver – DPO

Mail: DPO@herningsholm.dk
Telefon: +45 2542 4824 (Peter)
eller +45 2542 4818 (Helle

Databeskyttelsesrådgiverens rolle, opgaver og ansvar er uddybet i bilag 9 ”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.

VBCs databeskyttelsesrådgiver bistår Datatilsynet i forbindelse med tilsynssager og andre forespørgsler.

Se endvidere bilag 9 ”Retningslinje for databeskyttelsesrådgivere”.

Kontrol og dokumentation

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

Bilag 1: Retningslinje om god databehandlingsskik

Anvendelsesområde

Retningslinje om god databehandlingsskik 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 Vejen Business College (VBC), der behandler personoplysninger.

Formål

Formålet med denne retningslinje er at sikre, at VBC behandler personoplysninger i overensstemmelse med god databehandlingsskik.

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.

Almindelige/fortrolige personoplysninger er alle oplysninger om en identificeret eller identificerbar person, der ikke er omfattet af nedenstående kategori, eksempelvis navn, adresse, CPR-nummer, e-mail, billeder, telefonnummer.

Følsomme personoplysninger er oplysninger om helbredsforhold, fagforening, racemæssig eller etnisk baggrund, politisk, religiøs eller filosofisk overbevisning, seksuelle forhold og genetiske oplysninger.
Der er tale om en udtømmende liste.

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

God databehandlingsskik

VBC skal sikre, at vi behandler personoplysninger på en lovlig, rimelig og gennemsigtig måde.

- Lovlig henviser til, at VBC sikrer, at der er et lovligt hjemmelsgrundlag, se endvidere *retningslinje om behandlingsgrundlag*.

- Rimelig henviser til, at VBC kun må behandle personoplysninger, hvis behandlingens formål med rimelighed ikke kan opfyldes på anden måde.

- Gennemsigtig indebærer, at VBC skal oplyse den registrerede om den behandling, vi foretager om vedkommende. Behandlingen af personoplysninger skal således ske på en åben og oplyst måde.

Formålsbegrænsning

Når der indsamles oplysninger, skal VBC gøre sig klart, hvilke formål oplysningerne indsamles til, og det skal være saglige formål. Vi må således ikke indsamle oplysninger med den begrundelse, at det *måske* senere kan vise sig nyttigt at være i besiddelse af oplysningerne.

Dataminimering

Når VBC behandler personoplysninger, skal vi sikre, at behandlingen begrænses til det, der er nødvendigt for at opfylde formålet.

Vi skal således vurdere, om den konkrete behandling kan opfyldes ved at behandle færre personoplysninger.

Opbevaringsbegrænsning

Personoplysninger skal slettes eller gøres anonyme, når det ikke længere er nødvendigt for VBC at have oplysningerne.

Integritet og fortrolighed

VBC skal beskytte oplysningerne mod uautoriseret eller ulovlig behandling, ligesom det skal sikres, at oplysninger ikke går tabt eller bliver beskadiget. Dette sikrer vi ved at etablere passende tekniske og organisatoriske sikkerhedsforanstaltninger

VBC må således ikke behandle personoplysninger, førend det er sikret, at der er tilstrækkelig sikkerhed til stede ved behandlingen.

Kontrol og dokumentation

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

VBC dokumenterer

- At vi har et lovligt formål med behandlingen af personoplysninger
- At vi overholder kravene til god databehandlingsskik
- At den løbende kontrol overholdes

Bilag 2: Retningslinje om behandlingsgrundlag

Anvendelsesområde

Retningslinje om behandlingsgrundlag 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 Vejen Business College (VBC), der behandler personoplysninger.

Formål

Formålet med denne retningslinje er at sikre, at VBC udelukkende behandler personoplysninger på baggrund af et lovligt grundlag.

Bestyrelsen for VBC er ansvarlige for at ovenstående overholdes.

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.

Almindelige/fortrolige personoplysninger er alle oplysninger om en identificeret eller identificerbar person, der ikke er omfattet af nedenstående kategori, eksempelvis navn, adresse, CPR-nummer, e-mail, billeder, telefonnummer.

Følsomme personoplysninger er oplysninger om helbredsforhold, fagforening, racemæssig eller etnisk baggrund, politisk, religiøs eller filosofisk overbevisning, seksuelle forhold og genetiske oplysninger. Der er tale om en udtømmende liste.

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 VBC. Databeskyttelsesrådgiverens funktion er at understøtte, at VBC overholder reglerne i forordningen.

Behandlingsgrundlag

Behandlingsgrundlagene afhænger af hvilken type oplysning der behandles – *almindelige personoplysninger* eller *følsomme personoplysninger*.

VBCs databeskyttelsesrådgiver kan vejlede omkring det rette behandlingsgrundlag

Kontaktoplysninger på databeskyttelsesrådgiver:

Databeskyttelsesrådgiver – DPO

Mail: DPO@herningsholm.dk
Telefon: +45 2542 4824 (Peter)
eller +45 2542 4818 (Helle

VBC dokumenterer altid hvilket hjemmelsgrundlag en behandling af personoplysninger er sket på baggrund af.

Behandlingsgrundlag for almindelige/fortrolige personoplysninger

Når VBC behandler almindelige/fortrolige personoplysninger skal vi sikre, at behandlingen bygger på ét af nedenstående behandlingsgrundlag:

Samtykke fra den registrerede
(databeskyttelsesforordningens artikel 6, stk. 1 litra a)

VBC må behandle almindelige personoplysninger, hvis den registrerede har givet samtykke til behandling af sine personoplysninger til ét eller flere formål.

Det skal sikres, at samtykket er afgivet som en frivillig, specifikt, informeret og utvetydig viljeserklæring.

Det indebærer, at

- Samtykket ikke må være afgivet under nogen former for tvang
- Samtykket skal være så specifikt beskrevet, at det er tydeligt for den registrerede, hvad denne samtykker til
- Samtykket skal afgives som en aktiv handling

VBC skal kunne påvise, at den registrerede har afgivet sit samtykke, hvorfor samtykket bør være skriftligt.

VBC oplyser altid den registrerede om, hvordan denne tilbagetrækker sit samtykke. I tilfælde af at den registrerede trækker sit samtykke tilbage, stopper VBC fremadrettet den behandling af personoplysninger, der sker på baggrund af den registreredes samtykke.

Tilbagetrækning af samtykke skal ske til VBCs databeskyttelsesrådgiver.

Nødvendig behandling af hensyn til opfyldelse af en kontrakt
(databeskyttelsesforordningens artikel 6, stk. 1 litra b)

VBC kan behandle almindelige personoplysninger, hvis det er nødvendigt for os af hensyn til indgåelse eller opfyldelse af en kontrakt, som den registrerede er en del af.

Det kan eksempelvis være relevant i forbindelse med en ansættelseskontrakt eller ved optag af elever.

Behandling er nødvendig for overholdelse af retlig forpligtelse
(databeskyttelsesforordningens artikel 6, stk. 1, litra c)

VBC kan behandle almindelige personoplysninger, hvis vi er forpligtet hertil i henhold til lovgivningen.

Det vil eksempelvis være relevant, når VBC behandler personoplysninger i relation til elevers SU, eller når vi indberetter lønoplysninger til SKAT.

Behandling er nødvendig for overholdelse af den registreredes vitale interesse
(databeskyttelsesforordningens artikel 6, stk. 1, litra d)

VBC kan behandle almindelige personoplysninger, når det er nødvendigt for at beskytte den registreredes eller en anden fysisk persons vitale interesser.

Dette kan eksempelvis være relevant, hvis en ansat eller en elev besvimer på en studietur, hvorefter skolen kontakter et familiemedlem.

Behandling på baggrund af dette hjemmelsgrundlag bør kun finde sted, hvis behandlingen tydeligvis ikke kan baseres på et andets retsgrundlag.

Behandling er nødvendig af hensyn til udførelse af opgave i samfundets interesse eller som henhører under offentlig myndighedsudøvelse, som den dataansvarlige er blevet pålagt
(databeskyttelsesforordningens artikel 6, stk. 1, litra e)

I henhold til denne bestemmelse kan VBC behandle almindelige personoplysninger, når det er i samfundets interesse.

Udtrykket "opgave i samfundets interesse" indebærer, at der skal være tale om opgaver af almen interesse – dvs. opgaver, der har betydning for en større kreds af mennesker.

Endvidere kan vi behandle personoplysninger på baggrund af denne bestemmelse, når behandlingen er nødvendig af hensyn til en opgave, der henhører offentlig myndighedsudøvelse.

Udførelse af opgaver, der karakteriseres som faktisk forvaltningsvirksomhed, vil efter omstændighederne være omfattet af denne bestemmelse, eksempelvis undervisning.

Behandlingsgrundlag for følsomme personoplysninger[1]

Når VBC behandler følsomme personoplysninger, skal vi sikre, at behandlingen bygger på ét af nedenstående behandlingsgrundlag:

Udtrykkeligt samtykke fra den registrerede
(databeskyttelsesforordningens artikel 9, stk. 2, litra a)

Lige som ved almindelige oplysninger, skal samtykket være afgivet som en frivillig, specifikt, informeret og utvetydig viljeserklæring.

[1] De nævnte hjemmelsgrundlag for behandling af følsomme oplysninger, er udvalgt på baggrund af skolens behandlingsaktiviteter.

Det indebærer, at

- Samtykket ikke må være afgivet under nogen former for tvang,
- Samtykket skal være så specifikt beskrevet, at det er tydeligt for den registrerede, hvad denne samtykker til
- Samtykket skal afgives som en aktiv handling

Når VBC behandler personoplysninger på baggrund af et samtykke fra den registrerede, sikrer vi os endvidere, at der er tale om et udtrykkeligt samtykke.

Udtrykkeligt samtykke henviser til, at VBC ikke opnår stiltiende eller indirekte accept fra den registrerede.

VBC skal kunne påvise, at den registrerede har afgivet sit samtykke, hvorfor samtykket bør være skriftligt.

VBC oplyser altid den registrerede om, hvordan denne tilbagetrækker sit samtykke. I tilfælde af at den registrerede trækker sit samtykke tilbage, stopper VBC fremadrettet den behandling af personoplysninger, der sker på baggrund af den registreredes samtykke.

Tilbagetrækning af samtykke skal ske til VBCs databeskyttelsesrådgiver.

Behandling er nødvendig for at overholde VBCs eller den registreredes arbejds-, sundheds- og socialretlige forpligtelser i henhold til særlovgivning
(databeskyttelsesforordningens artikel 9, stk. 2, litra b)

Når VBC behandler personoplysninger på baggrund af denne hjemmel, har vi bl.a. mulighed for at opretholde det arbejdsretlige bodssystem i relation til ulovlige arbejdskonflikter.

Benyttelsen af dette hjemmelsgrundlag skal ske med udgangspunkt i gældende arbejdsret – eksempelvis i overenskomster og andre anerkendte retskilder.

Behandling er nødvendig for overholdelse af den registreredes vitale interesse
(databeskyttelsesforordningens artikel 9, stk. 2, litra c)

VBC kan behandle almindelige personoplysninger, når det er nødvendigt for at beskytte den registreredes eller en anden fysisk persons vitale interesser.

Dette kan eksempelvis være relevant, hvis en ansat eller en elev besvimer på en studietur, hvorefter skolen kontakter et familiemedlem.

Behandling på baggrund af dette hjemmelsgrundlag bør kun finde sted, hvis behandlingen tydeligvis ikke kan baseres på et andets retsgrundlag, eksempelvis samtykke.

Behandling vedrører personoplysninger, der tydeligvis er offentliggjort af den registrerede.
(databeskyttelsesforordningens artikel 9, stk. 2, litra e)

VBC kan behandle følsomme personoplysninger, såfremt den registrerede tydeligvis har offentliggjort oplysningen selv.

Eksempelvis hvis den registrerede offentligt ytre, at denne er medlem af XX fagforening, eller lider af XX sygdom.

Selvom den registrerede har offentliggjort oplysningen, skal VBC behandle den følsomme personoplysning i overensstemmelse med forordningens regler, herunder de grundlæggende behandlingsprincipper i artikel 5.

Det bemærkes, at *offentliggjort* henviser til, at oplysningen er gjort tilgængelig for "enhver". Det vil således som udgangspunkt ikke gøre sig gældende hvis oplysningen lægges på en lukket facebookprofil.

Endvidere skal offentliggørelsen ske af den registrerede og må derfor ikke være på andres foranledning.

Kontrol og dokumentation

VBC skal sikre, at der løbende foretages en dokumenteret kontrol af, at denne retningslinje overholdes. Kontrollen skal godkendes af bestyrelsen for VBC.

VBC skal kunne dokumentere (påvise):

- Hvilket hjemmelsgrundlag vi bygger vores behandling af personoplysninger på
- Hvilket hjemmelsgrundlag i særlovgivning vi i givet fald bygger vores behandling af personoplysninger på
- At den løbende kontrol med denne retningslinje overholdes

Bilag 3: Retningslinje om overførsel til tredjelande

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 Vejen Business College (VBC), der behandler personoplysninger, samt for samarbejdspartnere (databehandlere), der udfører opgaver på vegne af VBC.

Formål

Formålet med denne retningslinje er at sikre, at VBC, 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 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, eksempelvis 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 eksempelvis 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 hos VBC. Databeskyttelsesrådgiverens funktion er at understøtte, at VBC overholder reglerne i forordningen.

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[2]. 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 VBC ikke kan overføre personoplysninger til et tredjeland, hvis dette tredjelands lovgivning, praksisser mv., ikke muliggør en efterlevelse af garantierne.

Hvad er en overførsel?

Begrebet "overførsel" dækker både over den situation, hvor VBC **videregiver** personoplysninger til en ny dataansvarlig i et tredjeland og den situation, hvor VBC **overlader** en behandling af personoplysninger til en databehandler i tredjeland.

En overførsel kan eksempelvis 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:

VBC 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.

[2] http://www.eu.dk/da/spoergsmaal-og-svar-folder/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 VBC 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 VBC 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[3].

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 VBC ønsker at overføre personoplysninger til et usikkert tredjeland, skal vi give de fornødne garantier for databeskyttelse. En fornøden garanti kan eksempelvis gives ved indgåelse af en kontrakt mellem VBC og dataimportøren (enten dataansvarlig eller databehandler i tredjelandet).

Nedenfor ses de muligheder som VBC har for at give de fornødne garantier:

1) Retligt bindende instrumenter (aftaler mv.) mellem offentlige myndigheder eller organer,
2) Bindende virksomhedsregler,
3) Adfærdskodeks og certificeringsmekanismer,
4) Standardbestemmelser om databeskyttelse

[3] https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en

5) Ad hoc-kontrakter.

Denne retningslinje gennemgår punkt 3 og 4.

Ad. Adfærdskodeks og certificeringsmekanismer:

VBC 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 eksempelvis opnås ved at få certificeret, at de it-løsninger VBC bruger, overholder kravene i databeskyttelsesforordningen.

Hvis en dataansvarlig eller en databehandler i et tredjeland tilslutter sig et godkendt adfærdskodeks eller en godkendt certificeringsordning, vil VBC 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 indenfor 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:

1. Adfærdskodekset eller certificeringsordningen skal være godkendt af den kompetente tilsynsmyndighed eller af et certificeringsorgan.
2. Adfærdskodekset eller certificeringsordningen skal indeholde specifikke regler om tredjelandsoverførsel.
3. Der skal foreligge et bindende tilsagn fra dataimportøren (dataansvarlig/databehandler) i et tredjeland om at anvende adfærdskodekset eller certificeringsordningens regler om tredjelandsoverførsel.
4. Det bindende tilsagn skal kunne håndhæves af et kompetent kontrolorgan.

Se endvidere databeskyttelsesforordningens artikel 40-43.

Ad. 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 VBC 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 kan findes på Kommissionens hjemmeside: https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en.

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 VBC, som dataansvarlig, forpligtet til at indgå en standardkontrakt direkte med underdatabehandleren.[4]

Hvis VBC 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".

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

Kontrol og dokumentation

VBC skal sikre, at vi løbende foretager en dokumenteret kontrol af, at denne retningslinje overholdes. Kontrollen skal godkendes af VBCs bestyrelse.

VBC dokumenterer:

- At vi har et overblik over vores overførsler til tredjelande
- At vi har de fornødne overførselsgrundlag
- At vi, foruden et overførselsgrundlag, indgår databehandleraftaler med vores eventuelle databehandlere i tredjelande

[4] Dette gør sig udelukkende gældende i forbindelse med første led af underdatabehandlere. Såfremt underdatabehandleren gør brug af en under-underdatabehandler, 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.

Bilag 1 - Kvikguide til tredjelandsoverførsler

1. Tredjelandsoverførsel?

Overvej om de pågældende oplysninger er personoplysninger, om der sker en overførsel, om overførslen sker til et tredjeland og om de fire essentielle europæiske garantier overholdes.

- Hvis dette er tilfældet, så gå videre til næste boks

2. Iagttagelse af forordningen?

Overvej om alle forordningens regler overholdes inden tredjelandsoverførsel påtænkes.

- Hvis dette er tilfældet, så gå videre til næste boks.

3. Overførsel til sikre tredjelande?

Undersøg om tredjelandet er vurderet af Kommissionen som sikkert.

- Hvis dette er tilfældet, kan oplysningerne uden videre overføres.

- Hvis dette ikke er tilfældet, så gå videre til næste boks.

4. Overførsel til usikre tredjelande?

Undersøg om der er fastsat fornødne garantier for tredjelandsoverførslen.

- Hvis dette er tilfældet, kan overførslen lovligt ske.

- Hvis dette ikke er tilfældet, kan overførslen ikke ske

Bilag 4: Retningslinje om fortegnelser over behandlingsaktiviteter

Anvendelsesområde

Retningslinje om fortegnelser over behandlingsaktiviteter 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 Vejen Business College (VBC), der behandler personoplysninger, samt for samarbejdspartnere (databehandlere), der udfører opgaver på vegne af VBC.

Formål

Formålet med denne retningslinje er at sikre, at VBC fører de lovpligtige fortegnelser over behandlingsaktiviteter, som efter anmodning skal stilles til rådighed for Datatilsynet. Fortegnelserne kan ligeledes anvendes som hjælp til at sikre, at der foreligger et grundlag for vurdering af risici for behandling af personoplysninger.

Fortegnelserne skal som hovedregel laves på hovedformålsniveau – eksempelvis "personaleadministration". Der kan dog være fordele ved at nedbryde fortegnelserne i delformål – eksempelvis "ansættelse", "under ansættelsesforholdet" og "efter ansættelsesophør".

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

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.

Den dataansvarliges fortegnelse over behandlingsaktiviteter

I henhold til forordnings artikel 30, stk. 1, skal VBC, når vi er dataansvarlige myndighed, føre en fortegnelse over vores behandlingsaktiviteter – dvs. en fortegnelse over såvel almindelige som følsomme personoplysninger.

VBCs fortegnelse skal som minimum indeholde kontaktoplysninger på VBC samt vores databeskyttelsesrådgiver. Hvis vi er fælles dataansvarlige med en anden dataansvarlig, skal denne dataansvarlig ligeledes fremgå af fortegnelsen.

I fortegnelsen skal der være en beskrivelse af formålet med databehandlingen. Det kan i mange tilfælde være muligt at samle flere behandlingsaktiviteter i ét sammenhængende logisk formål – eksempelvis ”sagsbehandling” eller ”personaleadministration”.

Fortegnelsen skal give et klart overblik over hvilke personoplysningskategorier vi behandler, eksempelvis ”identifikationsoplysninger”, ”billeder”, ”helbredsoplysninger”. Derudover skal vi beskrive hvilke kategorier af registrerede vi behandler personoplysninger om, eksempelvis ”ansatte”, ”elever” og /eller ”forældre”.

Hvis VBC får hjælp til at behandle personoplysninger af en databehandler eller hvis vi videregiver personoplysninger til en ny dataansvarlig, skal dette fremgå af fortegnelsen. Her skal det også beskrives, hvorvidt oplysningerne overlades/videregives til lande uden for EU, ligesom det skal fremgå hvad hjemmelsgrundlaget for overladelsen/videregivelsen er.

I videst muligt omfang skal VBC beskrive, hvornår vi påtænker at slette personoplysningerne igen, samt hvilke tekniske og organisatoriske foranstaltninger vi har indført for at mindske risikoen i forhold til den registreredes rettigheder og frihedsrettigheder, når vi behandler dennes oplysninger.

Se endvidere bilag 1, hvor kravene til dataansvarliges fortegnelse er oplistet.

Databehandlers fortegnelse over kategorier af behandlingsaktiviteter

Når VBC behandler personoplysninger på vegne af en anden dataansvarlig, er vi databehandlere.

I tilfælde af at VBC er databehandlere, er vi forpligtet til at føre en fortegnelse over alle de kategorier af behandlingsaktiviteter, som vi foretager på vegne af den dataansvarlige.

Fortegnelsen skal som minimum indeholde kontaktoplysninger på VBC samt kontaktoplysninger på den dataansvarlige, herunder dennes repræsentant og eventuelle databeskyttelsesrådgiver.

Som databehandlere er VBC udelukkende forpligtet til at føre en fortegnelse over de kategorier af behandlingsaktiviteter, som vi foretager på vegne af den dataansvarlige.

Hvis VBC får hjælp til at behandle personoplysninger af en underdatabehandler skal dette fremgå af fortegnelsen. Her skal det også beskrives, hvorvidt oplysningerne overlades til lande uden for EU, ligesom det skal fremgå, hvad hjemmelsgrundlaget for overladelsen er.

I videst muligt omfang skal VBC beskrive hvilke tekniske og organisatoriske foranstaltninger, vi har indført for at mindske risikoen i forhold til den registreredes rettigheder og frihedsrettigheder, når vi behandler dennes oplysninger på vegne af den dataansvarlige.

Se endvidere bilag 2, hvor kravene til databehandlers fortegnelse er oplistet.

Formkrav og opdatering

Fortegnelsen skal foreligge i skriftlig og elektronisk form.

Fortegnelsen skal opdateres løbende, således VBC altid på anmodning kan levere et korrekt overblik over vores behandlingsaktiviteter til Datatilsynet.

Kontrol og dokumentation

VBC skal sikre, at vi løbende foretager en dokumenteret kontrol af, at denne retningslinje overholdes. Kontrollen skal godkendes af bestyrelsen for VBC.

VBC skal kunne dokumentere (påvise), at:

- Fortegnelsen er udarbejdet, og at den opfylder minimumskravene, som beskrevet i denne retningslinje
- Fortegnelsen foreligger skriftligt og i elektronisk format
- Den løbende kontrol overholdes

Bilag 1:

Dataansvarliges fortegnelse over behandlingsaktiviteter

Den dataansvarliges fortegnelse skal som minimum indeholde følgende oplysninger:

a) Navn på og kontaktoplysninger på Vejen Business College og, hvis det er relevant, den fælles dataansvarlige, den dataansvarliges repræsentant og databeskyttelsesrådgiveren	Vejen Business Colleges navn og kontaktoplysninger skal oplyses samt databeskyttelsesrådgiverens navn og kontaktoplysninger.
b) Formålene med behandlingen	Samtlige formål med behandlingsaktiviteten skal fremgå – det gælder således også de behandlinger, som eventuelt foretages af en databehandler. Der skal formuleres et samlet logisk sammenhængende formål – eksempelvis "*personaleadministration*" eller "*sagsbehandling*"
c) En beskrivelse af kategorierne af registrerede og kategorierne af personoplysninger	Kategorier af registrerede: Eksempelvis "*ansatte*", "*elever*", "*tidligere ansatte*", "*forældre*". Kategorier af personoplysninger: Eksempelvis "*identifikationsoplysninger*","*lønoplysninger*", "*helbredsoplysninger*", "*fagforeningsmæssigt tilhørsforhold*"
d) De kategorier af modtagere, som personoplysningerne er eller vil blive videregivet til, herunder modtagere i tredjelande	Eksempelvis: "*Offentlige myndigheder – så vidt muligt myndighedens navn, såsom SKAT*", "*sociale medier*", "*banker*"
e) Hvor det er relevant, overførsler af personoplysninger til et tredjeland, herunder angivelse af dette tredjeland.	Her skal angives om Vejen Business College har samarbejdspartnere, der er etableret uden for EU. Eksempelvis "*Google*", "*Amazon*", "*Facebook*".
f) Hvis det er muligt, de forventede tidsfrister for sletning af de forskellige kategorier af oplysninger	Eksempelvis: "*Oplysninger om tidligere ansatte slettes 5 år efter fratrædelse".*
g) Hvis det er muligt, en generel beskrivelse af de tekniske og organisatoriske sikkerhedsforanstaltninger omhandlet i artikel 32, stk. 1.	Eksempelvis: "*Personoplysninger opbevares i krypteret og pseudonymiseret form og transmitteres krypteret.* *Fysisk materiale opbevares bag 2 låse*".

Bilag 2:

Databehandlers fortegnelse over kategorier af behandlingsaktiviteter

Databehandlers fortegnelse skal som minimum indeholde følgende oplysninger:

a) Navn på og kontaktoplysninger på Vejen Business College og for hver dataansvarlig, på hvis vegne Vejen Business College behandler personoplysninger, samt, hvis det er relevant, den dataansvarliges eller databehandlerens repræsentant og databeskyttelsesrådgiveren	Vejen Business Colleges navn og kontaktoplysninger skal oplyses samt databeskyttelsesrådgiverens navn og kontaktoplysninger.
b) De kategorier af behandlinger, Vejen Business College foretager på vegne af den enkelte dataansvarlige	Her beskrives hvilke databehandlinger, Vejen Business College foretager på vegne af den dataansvarlige.
c) Hvor det er relevant, overførsler af personoplysninger til et tredjeland, herunder angivelse af dette tredjeland.	Her skal angives om Vejen Business College har samarbejdspartnere, der er etableret uden for EU. Eksempelvis "*Google*", "*Amazon*", "*Facebook*".
d) Hvis det er muligt, en generel beskrivelse af de tekniske og organisatoriske sikkerhedsforanstaltninger omhandlet i artikel 32, stk. 1.	Eksempelvis: "*Personoplysninger opbevares i krypteret og pseudonymiseret form og transmitteres krypteret.* *Fysisk materiale opbevares bag 2 låse*".

Bilag 5: Retningslinje om de registreredes rettigheder

Anvendelsesområde

Retningslinje om de registreredes rettigheder 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 Vejen Business College (VBC), der behandler personoplysninger.

Formål

Formålet med denne retningslinje er at sikre, at VBC altid er i stand til at iagttage de registreredes rettigheder.

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 VBC. Databeskyttelsesrådgiverens funktion er at understøtte, at VBC overholder reglerne i forordningen.

De registreredes rettigheder

De personer, som VBC behandler personoplysninger om, har en række rettigheder i henhold til databeskyttelsesforordningen, som vi som dataansvarlig skal iagttage.

De registreredes rettigheder er

- Oplysningspligt (artikel 13 og 14)
- Ret til indsigt (artikel 15) Bilag B
- Ret til berigtigelse (artikel 16)
- Ret til sletning (artikel 17)
- Ret til begrænsning af behandling (artikel 18)
- Underretningspligt i forbindelse med berigtigelse eller sletning af personoplysninger eller begrænsning af behandling (artikel 19)
- Ret til dataportabilitet (artikel 20)
- Ret til indsigelse (artikel 21)
- Ret til ikke at være genstand for en afgørelse, der alene er baseret på automatisk behandling, herunder profilering (artikel 22)

Oplysningspligten adskiller sig fra de øvrige rettigheder, idet VBC som dataansvarlig skal sørge for at iagttage dette på eget initiativ, hvorimod de andre rettigheder skal iagttages efter anmodning fra den registrerede.

Selvom der er tale om en rettighed, er VBC således i forhold til oplysningspligten forpligtet til at iagttage denne uanset, om den registrerede har anmodet herom.

På dataansvarliges initiativ - oplysningspligten

(databeskyttelsesforordningens artikel 13 og 14)

Vi skelner altid mellem den situation, hvor VBC indsamler personoplysninger *hos den registrerede* og den situation, hvor VBC indsamler oplysninger om den registrerede *hos andre* end den registrerede.

Indsamling hos den registrerede (artikel 13)

Når VBC indsamler personoplysninger direkte hos den registrerede, skal vi opfylde vores oplysningspligt *samtidig* med indsamlingen.

Hvis den registrerede eksempelvis udfylder en blanket, og efterfølgende giver den til os, kan vi med fordel opfylde vores oplysningspligt i blanketten.

Oplysningspligten skal opfyldes i forbindelse med hvert databehandlingsformål.

Indsamling hos andre end den registrerede (artikel 14)

Personoplysninger indsamles hos andre end den registrerede, når VBC har fået personoplysningerne fra eksempelvis andre dataansvarlige, herunder andre offentlige myndigheder.

Opfyldelsen af denne oplysningspligt skal ske så tidligt som muligt efter indsamlingen af personoplysningerne hvilket betyder, at vi som hovedregel giver de påkrævede oplysninger til den registrerede *inden for 10 dage*.

Oplysningspligten skal opfyldes i forbindelse med hvert databehandlingsformål.

Efter anmodning fra den registrerede[5]

Ret til indsigt

(databeskyttelsesforordningens artikel 15)

Efter denne bestemmelse har den registrerede ret til at se de personoplysninger, som VBC behandler om den pågældende. Derudover har den registrerede ret til at modtage en række oplysninger, om de behandlinger, VBC foretager, hvori den registrerede optræder.

På baggrund heraf har den registrerede mulighed for at følge med i om de pågældende personoplysninger er korrekte og ajourførte, samt om behandlingen er lovlig.

Som offentlig myndighed kan VBC undlade at imødekommen indsigtsanmodning, hvis oplysninger kan undtages efter reglerne i offentlighedslovens §§ 19-29 og § 35.

Hvis den registrerede anmoder om indsigt, udleverer VBC en liste med beskrivelse af:

- Formålet med behandlingen af personoplysningerne
- Kategorier af personoplysninger, eksempelvis "helbredsoplysninger", kontaktoplysninger" mv.
- Modtagere af personoplysninger, som personoplysningerne videregives til
- Tidsrummet for databehandlingen, dvs. hvor lang tid VBC agter at gemme oplysningerne
- Retten til at bede VBC om at berigtige oplysninger
- Klageadgange til Datatilsynet
- Hvorfra oplysningerne stammer, såfremt de ikke er indsamlet hos den registrerede
- De fornødne garantier, som VBC har gjort i tilfælde af overførsel til 3.lande

Se bilag A "Indsigt i personoplysninger"

Hvis VBC modtager en indsigtsanmodning, der er meget omfangsrig, kan vi anmode den registrerede om en præcisering af anmodningen. Det bemærkes dog, at såfremt den registrerede ikke ønsker at præcisere anmodningen, må VBC ikke afvise anmodningen. I tilfælde heraf er vi forpligtet til at give indsigt i alle de pågældende personoplysninger.

Børn

Hvis en forældremyndighedshaver ønsker at få indsigt i hvilke personoplysninger, VBC behandler om den pågældendes barn, skal vi foretage en konkret vurdering af barnets modenhedsniveau. Udgangspunktet er, at unge selvstændigt kan bede om indsigt, når de er 15 år. VBC kan i visse tilfælde give svaret på anmodningen til såvel den unge som forældrene, men det vil bero på en konkret vurdering.

Kontakt VBCs DPO i tvivlstilfælde:

Databeskyttelsesrådgiver – DPO

Mail: DPO@herningsholm.dk
Telefon: +45 2542 4824 (Peter)
eller +45 2542 4818 (Helle)

[5] De nævnte rettigheder er udvalgt på baggrund af skolens behandlingsaktiviteter og arbejdsområder.

Ret til berigtigelse

(databeskyttelsesforordningens artikel 16)

Efter denne bestemmelse har den registrerede ret til at få forkerte personoplysninger om sig selv rettet, samt at få fuldstændiggjort ufuldstændige personoplysninger.

Det er vigtigt at bemærke, at VBC på trods af ovenstående, stadig har en selvstændig pligt til at ajourføre personoplysninger.

I de tilfælde, hvor VBC ikke er enige med den registrerede om, at oplysningerne er urigtige, er vi som udgangspunkt ikke forpligtet til at berigtige dem, eksempelvis hvis der ikke er enighed om et mødenotat. I så fald sørger vi for at lave en tilføjelse til de omstridte oplysninger, hvoraf det fremgår at der er uenighed om personoplysningernes rigtighed.

Visse sager, kan indeholde faglige eller subjektive vurderinger af en registreret, eksempelvis en forstanders faglige vurdering af en elev, som den registrerede ikke er enig i. I denne situation sørger vi for at lave en

tilføjelse til de omstridte oplysninger, hvoraf det fremgår at der er uenighed om personoplysningernes rigtighed.

VBC sørger for at underrette eventuelle databehandlere eller tredjemænd, som vi måtte have videregivet de urigtige oplysninger til, således denne ligeledes kan berigtige oplysningerne.

Se endvidere skabelon i bilag A og A1.

"Retten til at blive glemt"
(databeskyttelsesforordningens artikel 17)

Retten til at blive glemt indebærer, at en registreret, med visse undtagelser, har ret til at få slettet personoplysninger om sig selv.

For at få slettet oplysningerne skal følgende gøre sig gældende:

- Personoplysningerne er ikke længere nødvendige for at opfylde det formål, de oprindeligt er indsamlet til
- Den registrerede trækker sig samtykke tilbage
- Den registrerede gør indsigelse mod behandlingen, jf. artikel 21
- Behandlingen er ulovlig
- Personoplysningerne skal i henhold til lovgivningen slettes

Når VBC sletter oplysninger, skal vi sørge for, at personoplysningerne slettes endegyldigt; de må således ikke kunne genskabes. Hvis det er teknisk muligt, sletter vi også oplysningerne fra vores backup.

Det er vigtigt at bemærke, at vi godt kan behandle de samme personoplysninger til flere formål. Det er altså vigtigt, at der sker en formålsbestemt sletning.

Det bemærkes, at VBC på trods af ovenstående, stadig har en selvstændig pligt til at slette personoplysninger, som ikke længere er nødvendige have i relation til de formål, hvortil personoplysningerne behandles.

Retten til at blive glemt er således som udgangspunkt kun relevant, når en registreret person anmoder om sletning før det tidspunkt, som VBC har oplyst til den registrerede.

VBC sørger for at underrette eventuelle databehandlere eller tredjemænd, som vi måtte have videregivet personoplysningerne til, således denne ligeledes kan slette oplysningerne, i tilfælde af at vi skal imødekomme sletningsanmodningen.

Undtagelser til retten til at blive glemt

VBC er ikke forpligtet til at slette personoplysninger, som vi i medfør af vores offentlige myndighedsudøvelse er forpligtet til behandle, eksempelvis notater i henhold til offentlige myndigheders notatpligt, eller såfremt vi behandler personoplysningerne som led i overholdelsen af en retlig forpligtelse.

Ret til begrænsning af behandling
(databeskyttelsesforordningens artikel 18 og 19)

Efter denne bestemmelse har den registrerede i visse tilfælde ret til at få begrænset behandlingen af sine personoplysninger. Herefter må VBC ikke behandle den pågældendes personoplysninger på andre måder end opbevaring.

VBC skal begrænse behandlingen, hvis

- Den registrerede mener, at de personoplysninger, vi behandler, er forkerte
- Behandlingen er ulovlig, og den registrerede modsætter sig sletning, men anmoder om begrænsning af anvendelsen
- Oplysningerne er ikke længere nødvendige til den pågældende behandling, men de er nødvendige i forbindelse med fastlæggelse af retskrav
- Den registrerede har gjort indsigelse mod behandlingen

VBC kan kun foretage anden behandling end opbevaring, hvis vi får den registreredes samtykke eller hvis det er nødvendigt for at overholde vores forpligtelser i henhold til lovgivningen, eksempelvis offentlighedslovens regler om aktindsigt.

Når vi begrænser oplysningerne, kan vi eksempelvis gøre oplysningerne utilgængelige for brugerne i systemet eller flytte de omstridte oplysninger over i et andet behandlingssystem. Hvis oplysningerne er offentliggjort på VBCs hjemmeside, skal de midlertidigt fjernes.

VBC underretter den registrerede, databehandlere og eventuelle tredjemænd inden vi ophæver en begrænsning af behandling.

Ret til dataportabilitet
(databeskyttelsesforordningens artikel 20)

I visse tilfælde har den registrerede ret til at få udleveret de personoplysninger, som pågældende har givet til os. Personoplysningerne skal gives i et struktureret og maskinlæsbart format.

Formålet med dataportabilitet er, at give den registrerede en øget kontrol over sine personoplysninger.

For at få personoplysningerne udleveret skal

1. VBCs behandling være baseret på et samtykke eller nødvendig af hensyn til opfyldelsen af en kontrakt.
2. Den registrerede selv have givet VBC sine personoplysninger.

Retten til dataportabilitet finder ikke anvendelse, når behandlingen henhører under offentlig myndighedsudøvelse, som VBC er pålagt.

Hvis den registrerede anmoder om det, skal VBC overføre personoplysningerne til en anden dataansvarlig, såfremt det er teknisk muligt. Det kunne eksempelvis være fra VBC til en anden skole i tilfælde af skoleskift. I denne situation er VBC ansvarlig for at oplysningerne overføres sikkert og krypteret, således oplysningerne ikke kommer til uvedkommendes kendskab.

Hvis VBC skal modtage personoplysninger fra en anden dataansvarlig, er det vigtigt, at vi sikrer, at vi behandler de modtagne personoplysninger på et lovligt grundlag. Hvis vi vurderer, at vi har fået flere oplysninger end hvad vi har brug for, er vi forpligtet til at slette disse oplysninger, medmindre den registrerede beder os specifikt om at gemme dem.

Ret til indsigelse
(databeskyttelsesforordningens artikel 21)

Efter denne bestemmelse har den registrerede mulighed for at gøre indsigelse mod en ellers lovlig behandling af sine personoplysninger.

Retten til indsigelse gælder kun hvis behandlingen er nødvendig af hensyn til udførelse af opgave i samfundets interesse eller som henhører under offentlig myndighedsudøvelse[6].

Hvis VBC modtager en indsigelsesanmodning, skal vi således på ny vurdere, om behandlingen er lovlig. Hvis vi vurderer, at behandlingen fortsat er lovlig, skal vi forklare den registrerede dette.

Krav til opfyldelse af de registreredes rettigheder

Udgangspunktet er, at det er den dataansvarlige, der er ansvarlig for at iagttage de registreredes rettigheder. Der er dog ikke noget til hinder for, at den dataansvarlige uddelegerer opgaven til en databehandler, eksempelvis i databehandleraftalen.

Når VBC kommunikerer med en registreret, sker det altid skriftligt, med mindre den registrerede specifikt har anmodet om en mundtlig besvarelse. Endvidere sikrer vi os, at kommunikationen altid sker på en kortfattet, lettilgængelig og forståelig måde.

Hvis VBC modtager en anmodning fra den registrerede, skal vi uden unødig forsinkelse, og senest en måned efter modtagelsen af anmodningen, give den registreret svar. I særlige tilfælde kan denne frist forlænges i op til 3 måneder, såfremt der er ekstraordinære årsager hertil.

[6] Retten til indsigt gælder også ift. interesseafvejningsreglen, som dog ikke gælder for offentlige myndigheder.

Kontakt VBCs DPO i tvivlstilfælde:

Databeskyttelsesrådgiver – DPO

Mail: DPO@herningsholm.dk
Telefon: +45 2542 4824 (Peter)
eller +45 2542 4818 (Helle)

Hvis VBC efter behandlingen af anmodningen finder, at denne ikke kan imødekommes, giver vi en skriftlig begrundelse, og vi vedlægger ligeledes en klagevejledning til Datatilsynet.

VBC skal som udgangspunkt besvare anmodninger, der relaterer sig til de registreredes rettigheder, uden beregning. Dette kan fraviges, såfremt der er tale om gentagne anmodninger, der er "åbenbart grundløse eller overdrevne". I tilfælde heraf kan den dataansvarlige ligeledes nægte at besvare anmodningen.

Kontakt VBCs DPO i tvivlstilfælde.

Kontrol og dokumentation

VBC sikrer, at der løbende foretages en dokumenteret kontrol af, at denne retningslinje overholdes. Kontrollen skal godkendes af bestyrelsen for VBC.

VBC skal kunne dokumentere (påvise):

- Opfylder vores oplysningspligt
- Overholder den registreredes rettigheder
- At den løbende kontrol med denne retningslinje overholdes

Bilag A Skabelon – indsigt

Vejledning til brug af skabelonen

Dele af skabelonen skal kun anvendes i det omfang, teksten er relevant for jeres behandling af personoplysninger om den registrerede. I så fald er teksten/afsnittet opsat med en kursiv skrifttype. Det betyder f.eks., at punkt 2 kun skal anvendes, hvis I har en databeskyttelsesrådgiver. De steder, hvor teksten optræder således, er det hensigten, at dette udfyldes af jer som dataansvarlig.

Enkelte steder kan der i skabelonen forekomme ((tekst i dobbelt parentes)). Dette er en kommentar til dig, der benytter skabelonen, og bør fjernes fra den endelige udgave.

Indsigt i personoplysninger

Ved [e-mail/brev] af [angiv dato] har du anmodet om indsigt i de oplysninger, der behandles om dig hos Vejen Business College.

Vi forstår din henvendelse som en anmodning om indsigt efter databeskyttelsesforordningen artikel 15.

Vejen Business College kan oplyse, at vi behandler oplysninger om dig. En kopi af personoplysningerne vedlægges.

Herudover skal vi i anledning af din anmodning give dig en række oplysninger om vores behandling af dine personoplysninger. De oplysninger vi skal give dig er disse:

1. Formålene med behandlingen af dine personoplysninger
2. Kategorier af personoplysninger
3. Modtagere eller kategorier af modtagere
4. Modtagere i tredjelande, herunder internationale organisationer
5. Opbevaring af personoplysningerne
6. Hvor dine personoplysninger stammer fra
7. Automatiske afgørelser, herunder profilering
8. Ret til berigtigelse, sletning, begrænsning og indsigelse
9. Klage til Datatilsynet

I det vedlagte bilag A1 finder du en uddybning i forhold til de oplysninger, vi skal give dig.

Har du spørgsmål, er du velkommen til at kontakte os på tlf.nr. 7536 1311 eller mail mb@vejenbc.dk.

Med venlig hilsen

Vejen Business College

Bilag A1 – Uddybende oplysninger om vores behandling af dine personoplysninger

1. Formålene med behandlingen af dine personoplysninger

Vejen Business College behandler dine personoplysninger til følgende formål:

[Beskriv formål – der kan godt være flere].

2. Kategorier af personoplysninger

Vejen Business College behandler følgende kategorier af personoplysninger om dig:

[Beskriv kategori/kategorier af personoplysninger, som I behandler om den registrerede, herunder om de personoplysninger, I har indsamlet, er almindelige personoplysninger eller særlige kategorier af personoplysninger (følsomme personoplysninger)].

3. Modtagere eller kategorier af modtagere

Vejen Business College videregiver eller overlader dine personoplysninger til følgende modtagere:

[Beskriv hvis muligt konkret modtager/konkrete modtagere eller kategorier af modtagere, f.eks. "SKAT", "andre offentlige myndigheder" eller "databehandlere"].

4. Modtagere i tredjelande, herunder internationale organisationer

Vi overfører dine personoplysninger til modtagere uden for EU og EØS.

Det drejer sig om [indsæt modtagere i usikre tredjelande], som er beliggende i [indsæt usikre tredjelande].

Vejen Business College kan oplyse, at [indsæt oplysninger om de fornødne garantier i medfør af artikel 46 i forbindelse med overførslen].

5. Opbevaring af dine personoplysninger

Vejen Business College opbevarer dine personoplysninger i henhold til vores slettepolitik, som du kan se på vores hjemmeside www.vejenbc.dk under Fakta – Persondataforordningen.

((Hvis det ikke er muligt at fastsætte et konkret tidsrum brug i stedet teksten nedenfor))

Vejen Business College kan på nuværende tidspunkt ikke sige, hvor længe vi vil opbevare dine personoplysninger. Dog kan vi oplyse dig om, at vi vil lægge vægt på [beskriv kriterier der anvendes til at fastlægge tidsrum], når vi skal fastlægge, hvor længe dine oplysninger vil blive opbevaret.

6. Hvor dine personoplysninger stammer fra

((Skal kun udfyldes, hvis oplysningerne ikke indsamles hos den registrerede))

Oplysningerne om dig stammer fra:

[Beskriv hvorfra oplysningerne stammer].

8. Ret til berigtigelse, sletning, begrænsning og indsigelse

Nedenfor kan du læse om din ret til berigtigelse, sletning, begrænsning og indsigelse. Hvis du vil gøre brug af dine rettigheder skal du kontakte os.

Ret til berigtigelse (rettelse)

Du har ret til at få urigtige oplysninger om dig selv rettet. Du har også ret til at få dine oplysninger suppleret med yderligere oplysninger, hvis dette vil gøre dine personoplysninger mere fuldstændige og/eller ajourførte.

Ret til sletning

I visse tilfælde har du ret til at få slettet oplysninger om dig, inden tidspunktet for vores almindelige generelle sletning indtræffer.

Ret til begrænsning af behandling

Du har i visse tilfælde ret til at få behandlingen af dine personoplysninger begrænset. Hvis du har ret til at få begrænset behandlingen, må vi fremover kun behandle oplysningerne – bortset fra opbevaring – med dit samtykke, eller med henblik på at retskrav kan fastlægges, gøres gældende eller forsvares, eller for at beskytte en person eller vigtige samfundsinteresser.

Ret til indsigelse

Du har i visse tilfælde ret til at gøre indsigelse mod vores ellers lovlige behandling af dine personoplysninger. Du kan også gøre indsigelse mod behandling af dine oplysninger til direkte markedsføring.

Du kan læse mere om dine rettigheder i Datatilsynets vejledning om de registreredes rettigheder, som du finder på www.datatilsynet.dk.

9. Klage til Datatilsynet

Du har ret til at indgive en klage til Datatilsynet, hvis du er utilfreds med den måde, vi behandler dine personoplysninger på. Du finder Datatilsynets kontaktoplysninger på www.datatilsynet.dk.

Bilag 6: Retningslinje om risikovurderinger

Anvendelsesområde

Retningslinje om risikovurdering 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 Vejen Business College (VBC), der behandler personoplysninger.

Formål

Formålet med denne retningslinje er at sikre, at VBC foretager den fornødne risikovurdering ved behandling af personoplysninger.

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.

Almindelige/fortrolige personoplysninger er alle oplysninger om en identificeret eller identificerbar person, der ikke er omfattet af nedenstående kategori, eksempelvis navn, adresse, CPR-nummer, e-mail, billeder, telefonnummer.

Følsomme personoplysninger er oplysninger om helbredsforhold, fagforening, racemæssig eller etnisk baggrund, politisk, religiøs eller filosofisk overbevisning, seksuelle forhold og genetiske oplysninger. Der er tale om en udtømmende liste.

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.

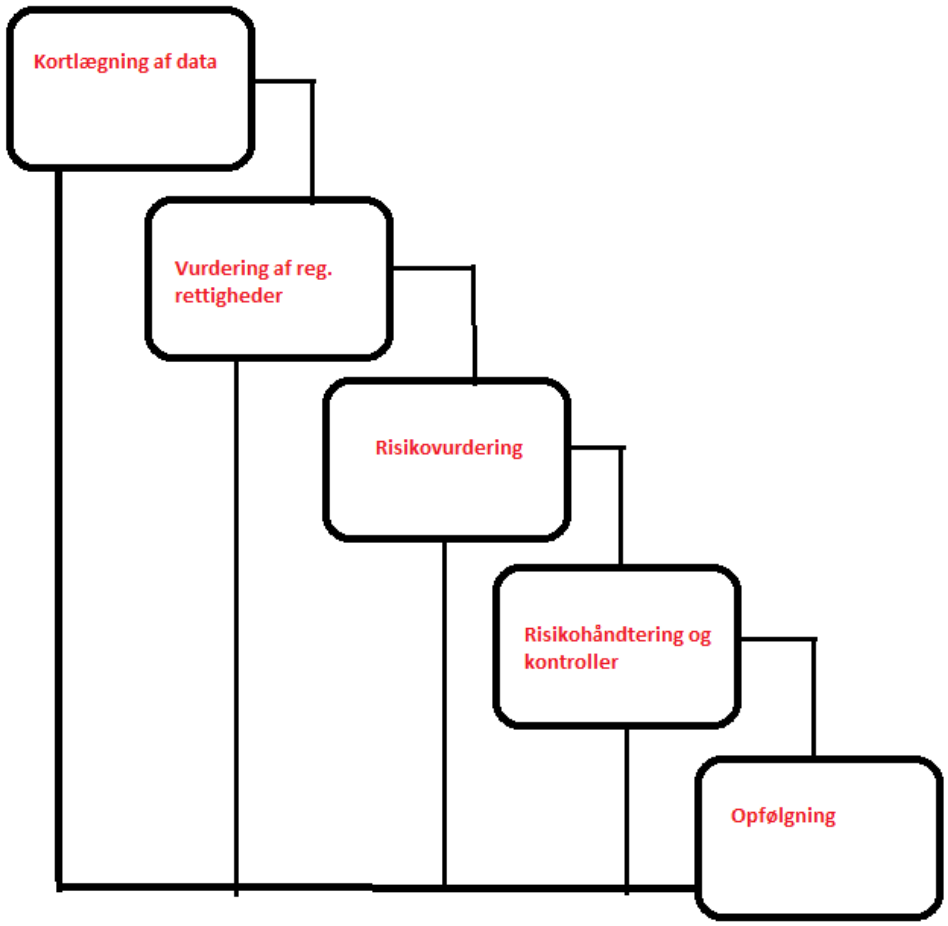
Databeskyttelsesrådgiveren (DPO) er en uafhængig person med ekspertise i databeskyttelsesret og –praksis, der skal inddrages i alle spørgsmål om databeskyttelse og rådgive om de databeskyttelsesretlige regler hos VBC. Databeskyttelsesrådgiverens funktion er at understøtte, at VBC overholder reglerne i forordningen.

Hvad er en risikovurdering?

En traditionel risikovurdering gennemføres ud fra den dataansvarliges eller systemansvarliges synspunkt. I en risikovurdering efter databeskyttelsesforordningen måles risikoen ved at bedømme, hvor stor sandsynlighed der er for, at en hændelse indtræffer, samt hvor store konsekvenser hændelsen kan have for den registrerede person og VBC. Det er den registrerede person, der er hovedfokus i denne risikovurdering.
En risikovurdering er således en vurdering af hvilke risici, der er forbundet med en konkret databehandling.
Ud fra den foretagne risikovurdering kan VBC gennemføre passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til de identificerede risici.

En risikoanalyse er tilmed et øjebliksbillede. Man får et indblik i, hvordan verden ser ud på det tidspunkt, hvor man gennemfører risikoanalysen.

Nedenfor ses en illustration af hele processen bag en risikovurdering.



Hvordan gør vi?

Når VBC foretager en risikovurdering, tager vi udgangspunkt i

- *Fareidentifikation*: En identifikation af hvilke hændelser, der kan ramme den registrerede.
- *Eksponeringsvurdering*: En vurdering af, hvor eksponeret VBC er for at blive påvirket af en bestemt hændelse i relation til den konkrete databehandling.

Ad. Fareidentifikation:
Fareidentifikationen skal vurderes ud fra den konkrete databehandling – eksempelvis:

"Ved anvendelse af system X til behandling af HR-oplysninger, er der risiko for at følgende hændelser indtræffer ……".

Ad. Eksponeringsvurdering:
Eksponeringsvurderingen skal give et indtryk af, hvor eksponeret VBC er for, at ovenstående hændelser vil indtræde.

En risikovurdering skal udføres af de personer, som har den nødvendige faglige indsigt.

Hvordan håndterer vi de identificerede risici?

Hvis VBC vurderer, at der kan være risici forbundet med en databehandling, skal vi efterfølgende afgøre, hvordan vi vil håndtere de identificerede risici. Vi skal således udarbejde en handlingsplan.

Der er som udgangspunkt fire muligheder for at håndtere risici:

1. Acceptér (risikoen accepteres, og der foretages ikke yderligere).
2. Flyt (den pågældende behandling flyttes – eksempelvis til et andet system).
3. Undgå (risikoen undgås ved at stoppe eller ændre den aktivitet, som er årsag til risikoen).
4. Kontrollér (risikoen kontrolleres ved at indføre foranstaltninger, som fjerner eller reducerer sandsynligheden eller konsekvenserne).

Det handler således om at prioritere og vælge sikkerhedsforanstaltninger, således vi nedbringer risici til et niveau, som er acceptabelt for såvel den registrerede som for skolen.

Formkrav

For at kunne overholde vores dokumentationsforpligtelse udfører vi risikovurderingen i skriftlig form.

Risikovurderingen opbevares sammen med øvrig behandlings dokumentation.

Kontrol og dokumentation

VBC skal sikre, at vi løbende foretager en dokumenteret kontrol af, at denne retningslinje overholdes. Kontrollen skal godkendes af bestyrelsen for VBC.

VBC skal kunne dokumentere (påvise):

- At vi foretager den fornødne risikovurdering, når vi igangsætter en behandling af personoplysninger
- At vi revurderer risikovurderingen, hvis behandlingen af personoplysninger ændrer karakter.
- At vi mindst én gang årligt gennemgår risikovurderingen
- At den løbende kontrol med denne retningslinje overholdes

Bilag 7: Retningslinje om behandlingssikkerhed

Anvendelsesområde

Retningslinje om behandlingssikkerhed 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 og gælder for alle ansatte på Vejen Business College (VBC), der behandler personoplysninger, samt for samarbejdspartnere (databehandlere), der udfører opgaver på vegne af VBC.

Formål

Formålet med denne retningslinje er at sikre, at VBC gennemfører de nødvendige sikkerhedsmæssige foranstaltninger, der modsvarer de identificerede risici for den registrerede, jf. databeskyttelses-forordningens artikel 25 og 32.

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, eksempelvis 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 eksempelvis 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 hos VBC. Databeskyttelsesrådgiverens funktion er at understøtte, at VBC overholder reglerne i forordningen.

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 behandlingssikkerhed?

Når VBC er dataansvarlig, er det vigtigt, at vi i tilstrækkelig grad beskytter de personoplysninger, som vi behandler.

Som dataansvarlig sikrer vi os således, at der tilvejebringes et sikkerhedsniveau der forhindrer, at der foretages databehandlinger i strid med forordningen, herunder at uvedkommende får adgang til personoplysningerne, at der sker sikkerhedsbrud eller at personoplysningerne anvendes til usalige formål.

Vi fastlægger sikkerhedsniveauet ud fra en samlet vurdering af det aktuelle tekniske niveau, implementeringsomkostninger og den pågældende databehandlings karakter, omfang, sammenhæng og formål samt risiciene og alvoren for fysiske personers rettigheder og frihedsrettigheder.

På baggrund af den samlede vurdering gennemfører VBC passende tekniske og organisatoriske foranstaltninger, således vi sikrer et sikkerhedsniveau, der passer til de identificerede risici, se endvidere *Retningslinje om risikovurdering*.

Beskyttelsesbehovet er større, jo mere følsomme personoplysningerne er. Derudover kan der være andre faktorer, der spiller ind i forbindelse med fastlæggelse af sikkerhedsniveauet, herunder risicienes varierende sandsynlighed samt mængden af data.

Hvis VBC i forbindelse med samme databehandling behandler såvel almindelige/fortrolige som følsomme oplysninger, tilpasser vi vores sikkerhedsforanstaltninger efter de mest følsomme personoplysninger.

Såfremt én af de sikkerhedsmæssige foranstaltninger, der fremgik af den tidligere gældende sikkerhedsbekendtgørelse, stadig er relevante, vil det være hensigtsmæssigt at benytte sig heraf, eksempelvis kravet om logning og autorisation.

Organisatoriske og tekniske foranstaltninger

Hvor den hidtidige persondatalov pålagde offentlige myndigheder at efterleve sikkerhedsbekendtgørelsen, foreskriver databeskyttelsesforordningen ikke hvilke foranstaltninger, der skal træffes for at imødekomme forordningens krav.

Lemvig Gymnasium vurderer således selv, hvordan vi løser opgaven med at skabe et tilstrækkeligt sikkerhedsniveau ud fra en risikovurdering.

Nedenfor forklares nogle af de mulige foranstaltninger.

Pseudonymisering

Ved pseudonymiserede personoplysninger forstås, at VBC behandler personoplysninger på en sådan måde, at de ikke længere direkte kan henføres til en bestemt person uden brug af supplerende oplysninger – en såkaldt omsætningsnøgle.

For at der er tale om pseudonymiserede personoplysninger, kræves det, at omsætningsnøglen opbevares særskilt, således det kun vil være udvalgte personer, der har adgang til omsætningsnøglen. Omsætningsnøglen er også underlagt kravet om tekniske og organisatoriske foranstaltninger.

Eksempel:

VBC erstatter de sidste 4 cifre i CPR-nummeret med en "kode", som kan genfindes på en separat liste, hvor man efterfølgende kan se koblingen mellem fødselsdagen og "koden", hvilket giver et personnummer.

Pseudonymiserede personoplysninger giver således en bedre beskyttelse af den registrerede person, idet det ikke umiddelbart er muligt at identificere personen.

Kryptering

Kryptering skal forstås således, at udvalgte personoplysninger gøres ulæselige ved hjælp af en krypteringsnøgle. For at tilgå de krypterede oplysninger, skal man være i besiddelse af den anvendte krypteringsnøgle.

Overførsel af almindelige og fortrolige personoplysninger via hjemmesider bør beskyttes ved kryptering.

Kommunikationen via hjemmesider kan sikres ved hjælp af SSL kryptering e.l. Der er mulighed for at implementere forskellige grader af kryptering, herunder også det, der betegnes som "stærk kryptering" (256 bit SSL/TLS-forbindelse).

Hvis brugere via hjemmesiden får adgang til personoplysninger – f.eks. om sig selv – skal der også skabes sikkerhed for, at oplysningerne ikke udleveres til uvedkommende. Dette kan eksempelvis ske ved anvendelse af adgangskode eller digital signatur. Hvis der gives adgang til følsomme personoplysninger, bør der anvendes digital signatur el.lign. (stærk kryptering).

Beredskab i tilfælde af en fysisk eller teknisk hændelse

VBC har nedsat et beredskab for, hvordan adgangen til personoplysninger genoprettes i tilfælde af fysiske eller tekniske hændelser, herunder eksempelvis brand, hacking, overgravede kabler mv.

Et beredskab handler om at planlægge, hvordan it-driften på baggrund af sådanne hændelser kan genoprettes inden for et nærmere bestemt tidsrum, samt hvordan vi bedst undgår en lignende hændelse – eksempelvis ved hjælp af regelmæssige sikkerhedskopier eller overgange til backupsystemer.

Afprøvning af procedure

VBC afprøver regelmæssigt vores firewalls, krypterede forbindelser, adgangskontroller, brugeradministrationsprocesser mv. med henblik på at sikre, at vi hele tiden er sikkerhedsmæssigt opdateret.

Organisatoriske foranstaltninger

Ved nogle ældre it-systemer, kan implementeringsomkostninger, der er forbundet med, at VBC f.eks. skal bringe systemet – der ikke på alle områder helt modsvarer det aktuelle tekniske niveau – op på et passende sikkerhedsniveau, være uforholdsmæssigt store. I disse tilfælde har VBC mulighed for at imødekomme behovet for større sikkerhed ved hjælp af organisatoriske foranstaltninger. Der er således ingen forpligtelse til at efterkomme sikkerhedskravene alene rent teknisk, hvis der efter en konkret vurdering findes tilstrækkelige organisatoriske løsninger, der også kan bidrage til at sikre det aktuelle tekniske niveau.

På baggrund af vores risikovurdering, etablerer VBC således passende organisatoriske foranstaltninger, herunder eksempelvis undervisning af medarbejdere, generelle oplysningskampagner (awareness) eller begrænsning af de medarbejdere, der har adgang til personoplysningerne.

Hvordan griber vi det praktisk an?

1. Identifikation og vurdering af risici

Inden VBC kan fastlægge, hvilke sikkerhedsforanstaltninger vi skal implementere, er det vigtigt, at vi foretager en risikovurdering, se endvidere *retningslinje om risikovurdering*.

2. Identifikation af mulige sikkerhedsmæssige foranstaltninger

Når VBC har identificeret og vurderet de risici, der kan være i forbindelse med en konkret databehandling, skal vi vurdere, hvilke foranstaltninger vi skal gennemføre, for at hindre at risiciene indtræffer.
Hvilke foranstaltninger der vil være mest hensigtsmæssige, afhænger af de aktuelle omstændigheder, herunder risici og omfang af databehandling, i forbindelse med den konkrete databehandling.

3. Implementering af foranstaltninger

Når VBC har identificeret de mulige sikkerhedsmæssige foranstaltninger, beslutter vi hvilke, som skal gennemføres for at etablere et sikkerhedsniveau, der passer til de identificerede risici.

Databeskyttelse gennem design

Ideen med databeskyttelsesforordningens artikel 25, stk.1 er, at et højt sikkerhedsniveau bedst sikres ved at implementere databeskyttelse i it-systemer allerede i systemudviklingen.

Ved databeskyttelse gennem design forventes det, at VBC tager højde for såvel de tekniske indretninger i systemet som vores organisatoriske arbejdsgange.

Kravet om databeskyttelse gennem design indebærer således, at VBC har en generel overvejelses- og håndteringsforpligtelse, hvilket betyder, at vi allerede i forberedelsesfasen skal overveje, indtænke og håndtere databeskyttelse i vores it-løsninger, således databeskyttelsesforordningen overholdes.

Eksempler på foranstaltninger, der kan indbygges fra start:

- Minimering af persondatabehandlingen (artikel 5, stk. 1, litra c),
- Pseudonymisering af personoplysninger (artikel 4, nr. 5, jf. Artikel 5, stk. 1, litra e),
- Transparens hvad angår personoplysningernes funktion og behandling (artikel 5, stk. 1, litra a),

- Kryptering af data i transit (artikel 5, stk.1, litra f jf. artikel 32, stk. 1, litra b)
- Sikring af infrastruktur mod uautoriseret indtrængen (artikel 5, stk.1, litra f jf. artikel 32, stk. 1, litra b)
- Organisatoriske kontroller til autorisation og styring af adgangsrettigheder (artikel 5, stk.1, litra f jfr. artikel 32, stk. 1, litra b)
- Udladelse af visning af oplysninger i brugergrænseflader, når disse ikke er nødvendige for en given behandling (artikel 5, stk. 1, litra f)

Databeskyttelse gennem standardindstillinger

I henhold til databeskyttelsesforordningen er VBC, som dataansvarlig, forpligtet til at sikre, at når eksempelvis softwareprogrammer, online-tjenester, it-systemer eller lignende anvendes til at behandle personoplysninger, skal de indstillingsmuligheder, som systemet mv. indeholder, som standard indstilles på en måde, der understøtter forordningens krav i artikel 25, stk. 2 om databeskyttelse gennem standardindstillinger.

Hvis systemet mv. giver mulighed for databeskyttelse, skal dette således indstilles som standard. Kravet om databeskyttelse gennem standardindstillinger kan ses som et påkrævet supplement til kravet om databeskyttelse gennem design.

Eksisterende it-systemer, hvor standardindstillingerne ikke kan ændres, vil ikke blive mødt af databeskyttelsesforordningens nye krav. Det forudsætter dog, at systemerne ikke forhindrer, at VBC lever op til databeskyttelsesforordningens krav, herunder eksempelvis kravene til behandlingssikkerhed i artikel 32 og de grundlæggende principper i artikel 5.

Når et it-system ændres, skal standardindstillingerne opfylde forordningens krav.

Når et eksisterende it-systems standardindstillinger kan ændres, vil VBC som dataansvarlig, være forpligtet til at tilpasse systemets standardindstillinger således, at disse understøtter forordningens krav om bl.a. formålsspecifik behandling.

Kontrol og dokumentation

VBC skal sikre, at vi løbende foretager en dokumenteret kontrol af, at denne retningslinje overholdes. Kontrollen skal godkendes af VBCs bestyrelse.

VBC skal kunne dokumentere (påvise), at:

- Der er tilvejebragt et sikkerhedsniveau, der svarer til de identificerede risici, der er forbundet med en konkret databehandling
- Der er nedsat et beredskab for, hvordan adgangen til personoplysningerne genoprettes i tilfælde af fysiske eller tekniske hændelser, herunder eksempelvis brand, hacking, overgravede kabler mv.
- Beredskabet afprøves regelmæssigt
- Der indtænkes databeskyttelse fra start ved implementering af nye it-systemer mv.
- De it-systemer mv., der giver mulighed for det, tilpasses sikkerhedsmæssigt, således databeskyttelse indstilles som standard.

Kontroller kan eksempelvis ske ved kvartalsvise stikprøvekontroller.

Bilag 8: Retningslinje om brud på persondatasikkerheden

Anvendelsesområde

Retningslinje om brud på persondatasikkerheden 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 Vejen Business College (VBC), der behandler personoplysninger, samt for samarbejdspartnere (databehandlere), der udfører opgaver på vegne af VBC.

Formål

Formålet med denne retningslinje er at sikre, at VBC håndterer eventuelle brud på persondatasikkerheden korrekt og i overensstemmelse med forordningens krav. Dette indebærer bl.a., at der sker anmeldelse til Datatilsynet, og at den registrerede underrettes i de tilfælde, hvor det er påkrævet.

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, eksempelvis 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 eksempelvis 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 hos VBC. Databeskyttelsesrådgiverens funktion er at understøtte, at VBC overholder reglerne i forordningen.
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.

Hvordan håndterer vi et brud på persondatasikkerheden?

Det kan have omfattende konsekvenser for den registrerede, hvis et brud på persondatasikkerheden ikke håndteres på en passende og rettidig måde. Konsekvenserne kan eksempelvis være tab af kontrol over den registreredes personoplysninger, forskelsbehandling, identitetstyveri, finansielle tab, tab af omdømme eller andre betydelige økonomiske eller sociale konsekvenser for den berørte fysiske person.

Det skal derfor sikres, at VBC har en klar procedure for håndtering af brud på persondatasikkerheden, når vi er henholdsvis dataansvarlig og databehandler.

Når Vejen Business College er dataansvarlig

Hvis der sker et brud på persondatasikkerheden, skal VBC, som hovedregel, og senest inden for 72 timer fra vi er blevet bekendt med bruddet, anmelde det til Datatilsynet.

Såfremt VBC kan dokumentere, at det er *usandsynligt*, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder, skal der ikke ske anmeldelse til Datatilsynet.

Vi skal således foretage en risikovurdering af, hvad bruddet har haft af betydning for den registrerede.

I vurderingen af risikoen skal der tages udgangspunkt i de konsekvenser sikkerhedsbruddet kan have for den registrerede, samt hvad sandsynligheden for disse konsekvenser er.

Afhængigt af hvilken grad af risici vores risikovurdering kommer frem til, skal følgende procedurer følges:

Risici	**Procedure**
Bruddet indebærer ingen risiko for den registrerede	Ej anmeldelsespligt til Datatilsynet
Bruddet indebærer en risiko for den registrerede	Anmeldelsespligt til Datatilsynet
Bruddet indebærer en *høj* risiko for den registrerede	Anmeldelsespligt til Datatilsynet samt underretningspligt over for den registrerede.

Bruddet indebærer ingen risiko for den registrerede:

I de tilfælde hvor den udførte risikovurdering viser, at det er usandsynligt, at bruddet på persondatasikkerheden har indebåret en risiko for den registreredes rettigheder, er bruddet ikke anmeldelsespligtigt til Datatilsynet.

Bruddet indebærer en risiko for den registrerede

Hvis risikovurderingen viser, at sikkerhedsbruddet indebærer en risiko for den registrerede, er VBC forpligtet til at anmelde bruddet til Datatilsynet. Anmeldelsen skal ske hurtigst muligt, og senest 72 timer fra VBC er blevet bekendt med bruddet.

Anmeldelsen til Datatilsynet skal som minimum indeholde:

1. Beskrivelse af karakteren af bruddet, samt hvor det er muligt;
    a. Kategorier af registrerede
    b. Antal af berørte registrerede
    c. Kategorier af personoplysninger
    d. Antal af berørte registreringer af personoplysninger
2. Navn og kontaktoplysninger på VBC databeskyttelsesrådgiver
3. Beskrivelse af mulige konsekvenser af sikkerhedsbruddet
4. Beskrivelse af de tekniske og organisatoriske foranstaltninger, som VBC har truffet eller foreslår truffet for at mindske skaden.

Se endvidere bilag 1, som indeholder en skabelon til brug for anmeldelse.

Bruddet indebærer en høj risiko for den registrerede

I de tilfælde hvor den udførte risikovurdering viser, at bruddet på persondatasikkerheden har indebåret en *høj* risiko for den registreredes rettigheder, skal bruddet anmeldes til Datatilsynet og de registrerede skal desuden, som hovedregel, underrettes – se dog undtagelser for underretning nedenfor.

Hvis det skulle ske, at vi i vores risikovurdering er nået frem til, at bruddet ikke indebærer en høj risiko for den registrerede, kan vi i visse tilfælde alligevel blive pålagt at underrette den registrerede, såfremt Datatilsynet i deres undersøgelse af bruddet vurderer, at der har været tale om en høj risiko.

Anmeldelsen til Datatilsynet skal som minimum indeholde:

1. Beskrivelse af karakteren af bruddet, samt hvor det er muligt;
    a. Kategorier af registrerede
    b. Antal af berørte registrerede
    c. Kategorier af personoplysninger
    d. Antal af berørte registreringer af personoplysninger
2. Navn og kontaktoplysninger på VBCs databeskyttelsesrådgiver
3. Beskrivelse af mulige konsekvenser af sikkerhedsbruddet
4. Beskrivelse af de tekniske og organisatoriske foranstaltninger, som VBC har truffet eller foreslår truffet for at mindske skaden.

Anmeldelsen kan sendes til dt@datatilsynet.dk eller via Datatilsynets hjemmeside.

Se endvidere bilag 1, som indeholder en skabelon til brug for anmeldelse.

Underretningen til den registrerede skal som minimum indeholde:

1. Beskrivelse af karakteren af bruddet
2. Navn og kontaktoplysninger på VBCs databeskyttelsesrådgiver
3. Beskrivelse af mulige konsekvenser af sikkerhedsbruddet
4. Beskrivelse af de tekniske og organisatoriske foranstaltninger, som VBC har truffet eller foreslår truffet for at mindske skaden.

Se endvidere bilag 2, som indeholder en skabelon til brug for underretning af den registrerede.

Situationer hvor Vejen Business College, på trods af høj risiko, ikke er forpligtet til at underrette den registrerede.

Én af følgende betingelser skal være opfyldt:

1. VBC har gennemført passende tekniske og organisatoriske beskyttelsesforanstaltninger, og disse foranstaltninger er blevet anvendt på de personoplysninger, som er berørt af bruddet på persondatasikkerheden, navnlig foranstaltninger, der gør personoplysningerne uforståelige for enhver, der ikke har autoriseret adgang hertil, som f.eks. kryptering
2. VBC har efter bruddet truffet foranstaltninger, der sikrer, at den høje risiko for den registreredes rettigheder sandsynligvis ikke længere er reel
3. Det vil kræve en uforholdsmæssig indsats. I et sådant tilfælde skal der i stedet foretages en offentlig meddelelse eller tilsvarende foranstaltning, hvorved den registrerede underrettes på en tilsvarende effektiv måde.

Databeskyttelsesrådgiveren

VBCs databeskyttelsesrådgiver inddrages altid, når der sker et brud på persondatasikkerheden.

Når Vejen Business College er databehandler

I de tilfælde, hvor VBC er databehandler for en anden dataansvarlig, underretter vi, uden unødig forsinkelse, den dataansvarlige efter at være blevet opmærksom på, at der er sket et brud på persondatasikkerheden.

Det er vigtigt, at VBC ligeledes instruerer vores databehandlere i, at underrette VBC, såfremt der skulle ske et brud på persondatasikkerheden.

Fortegnelse over sikkerhedsbrud

VBC er forpligtet til at dokumentere alle brud på persondatasikkerheden. Efter anmodning fra Datatilsynet, skal vi udlevere denne dokumentation.

Dokumentationen skal som minimum indeholde følgende:

1. Beskrivelse af karakteren af bruddet, samt hvor det er muligt;
    a. Kategorier af registrerede
    b. Antal af berørte registrerede
    c. Kategorier af personoplysninger
    d. Antal af berørte registreringer af personoplysninger
2. Navn og kontaktoplysninger på VBCs databeskyttelsesrådgiver
3. Beskrivelse af mulige konsekvenser af sikkerhedsbruddet
4. Beskrivelse af de tekniske og organisatoriske foranstaltninger, som VBC har truffet eller foreslår truffet for at mindske skaden.
5. Dokumentation for anmeldelse til Datatilsynet og evt. underretning til den registrerede.

Kontrol og dokumentation

VBC skal sikre, at vi løbende foretager en dokumenteret kontrol af, at denne retningslinje overholdes. Kontrollen skal godkendes af VBCs bestyrelse.

VBC skal kunne dokumentere (påvise), at:

- Vi foretager den nødvendige risikovurdering i forhold til den registreredes rettigheder
- Vi anmelder brud på persondatasikkerheden i de tilfælde, hvor det er påkrævet
- Anmeldelsen indeholder de minimumskrav, som forordningen stiller
- Vi underretter den registrerede om brud persondatasikkerheden i de tilfælde, hvor bruddet har indebåret en høj risiko for den registrerede
- Vi har instrueret vores databehandlere i at underrette os, hvis der sker et brud
- Vi overholder den løbende kontrol

Bilag 1: skabelon til anmeldelse til Datatilsynet

Dataansvarliges sagsnr.: [xxx]

Navn på dataansvarlig og dennes databeskyttelsesrådgiver

Organisationsnavn	[Indsæt skole]
CVR / EAN	[xxx]
Adresse	[xxx]
Kontaktperson	[xxx]
Telefon	[xxx]
E-mail	[xxx]

Involverede databehandlere

Databehandler

Organisationsnavn	[xxx]
CVR / EAN	[xxx]
Adresse	[xxx]

Underdatabehandler 1

Organisationsnavn	[xxx]
CVR / EAN	[xxx]
Adresse	[xxx]

Underdatabehandler 2

Organisationsnavn	[xxx]
CVR / EAN	[xxx]
Adresse	[xxx]

Beskrivelse af sikkerhedsbruddet

Beskrivelse af karakteren af bruddet, herunder kategorier af personoplysninger, behandlinger og antal af berørte registrerede

Har bruddet eksponeret følsomme personoplysninger for den registrerede?

Konsekvensanalyse af sikkerhedsbrud

Beskrivelse af sandsynlige konsekvenser for den registrerede ved bruddet på persondatasikkerheden

Mitigerende foranstaltninger

Beskrivelse af de foranstaltninger, som [indsæt skole] foreslår eller har iværksat for at afhjælpe bruddet på persondatasikkerheden

Bilag 2: skabelon til underretning af registrerede

[xx.xx.xxxx]

Kære [xxx]

Vi må desværre meddele dig, at [indsæt skole] [den xx.xx.xxxx] har fået kompromitteret vores persondatasikkerhed. Dette sikkerhedsbrud er allerede anmeldt til Datatilsynet, under sagsnr.: [DT-00193].

Beskrivelse af sikkerhedsbrud

[Indsæt beskrivelse, eksempelvis: "en af vore medarbejdere har ved en fejl delt et udtræk af personoplysninger fra et af vores kernesystemer med en ekstern. Dette udtræk inkluderede oplysninger om dig på følgende områder]:

[Indsæt kategorier, eksempelvis:]

- Navn
- Adresse
- Telefonnummer
- Fødselsdato
- CPR-nummer
- Etnisk oprindelse
- Land for pasudstedelse
- Pasnummer

Vi behandler dine personoplysninger, som led i at kunne [indsæt formål].

Konsekvenser for din person ved sikkerhedsbruddet

Da sikkerhedsbruddet indeholder [følsomme oplysninger] om dig, gør vi dig opmærksom på, at det vil kunne indebære at offentligheden kan have fået adgang til dine personoplysninger.

Foranstaltninger for at afhjælpe bruddet på persondatasikkerheden

Vi har allerede nu sørget for at [indsæt konkrete foranstaltninger – eksempelvis "destruere alle versioner af de pågældende udtræksfiler der ligger inden for grænserne af vores organisation. Den eksterne person, som data har været delt med er også blevet kontaktet og har slettet sin version af oplysningerne. Oplysningerne har imidlertid i kort tid været delt på et online fildrev, og vi er pt. i dialog med udbyderen for at sikre at data også er fjernet i eventuelle backupper, samt at høre om de har været udsat for nogen former for kriminalitet i det tidsrum, hvor data har eksisteret på deres servere".

Yderligere informationer og kontakt til os

Såfremt du har yderligere spørgsmål til kompromitteringen af dine personoplysninger, beder vi dig venligst tage kontakt til vores databeskyttelsesrådgiver:

Kontaktperson	[xxx]
Telefon	[xxx]
E-mail	dpo@herningsholm.dk

Endnu engang må vi beklage den risiko, vi har udsat dig for.

På vegne af [indsæt skole]

[XXX]

Bilag 9: Retningslinje om databeskyttelsesrådgivere

Anvendelsesområde

Retningslinje om databeskyttelsesrådgivere 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 Vejen Business College (VBC), der behandler personoplysninger.

Formål

Formålet med denne retningslinje er at redegøre for forordningens krav om udpegelse af databeskyttelsesrådgivere, samt dennes opgaver, kvalifikationer, stilling og inddragelse.

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 VBC. Databeskyttelsesrådgiverens funktion er at understøtte, at VBC overholder reglerne i forordningen.

Hvem skal have en databeskyttelsesrådgiver?

Offentlige myndigheder

I det omfang behandling foretages af en offentlig myndighed skal myndigheden altid have en databeskyttelsesrådgiver, hvad enten de er dataansvarlige eller databehandlere.

Det betyder, at der også skal udpeges en databeskyttelsesrådgiver, hvis den offentlige myndighed behandler personoplysninger på vegne af en privat eller selv outsourcer sin databehandling til en privat, som ikke er forpligtet til at udpege en databeskyttelsesrådgiver.

Hvornår er man en offentlig myndighed?

I forhold til selvejende institutioner m.v. oprettet på privatretligt grundlag, vil der således være nogle, som omfattes af kravet om at have en databeskyttelsesrådgiver, mens andre ikke omfattes. Det vil bero på en konkret vurdering.

Selvejende institutioner m.v. oprettet på privatretligt grundlag, som udøver offentlig virksomhed af mere omfattende karakter og er undergivet intensiv offentlig regulering, intensivt offentlig tilsyn og intensiv offentlig kontrol vil være omfattet.

Det spiller endvidere ind, om det offentlige har instruktionsbeføjelser over for institutionen, om det offentlige skal godkende institutionens vedtægter, og om det offentlige yder sekretariatsbistand.

Herudover må man se på, om det offentlige skal godkende institutionens regnskaber, og om institutionens drift og virksomhed er detaljeret reguleret ved regler og retningslinjer udstedt af det offentlige. Endelig kan man tage hensyn til, om det offentlige overtager institutionens rettigheder og forpligtelser, hvis den nedlægges.

Endvidere er det afgørende, om skolen er omfattet af forvaltningsloven og offentlighedsloven.

Eksempler på selvejende institutioner m.v., der er omfattet
- Universiteter
- Institutioner hvor kommunalbestyrelsen har indgået overenskomst til opfyldelse af sine forpligtelser efter lov om social service
- Gymnasieskoler

VBC er en selvejende offentlig virksomhed, hvorfor vi er forpligtet til at have en databeskyttelsesrådgiver.

Kontaktoplysninger til VBCs databeskyttelsesvejleder

Databeskyttelsesrådgiver – DPO

Mail: DPO@herningsholm.dk
Telefon: +45 2542 4824 (Peter)
eller +45 2542 4818 (Helle)

Konkret skal en virksomhed opfylde tre betingelser for at være forpligtet til at udpege en databeskyttelsesrådgiver:

1. Behandling af personoplysninger skal være virksomhedens kerneaktivitet
2. Der skal behandles personoplysninger i et stort omfang
3. Behandlingsaktiviteten består i regelmæssig og systematisk overvågning af personer eller behandlingen vedrører følsomme oplysninger eller oplysninger om strafbare forhold

Alle tre betingelser skal være opfyldt.

Hvem kan være databeskyttelsesrådgiver?

En databeskyttelsesrådgiver skal udpeges på baggrund af sine faglige kvalifikationer. Dette gælder navnlig evnen til at udføre sine opgaver som databeskyttelsesrådgiver og ekspertise inden for databeskyttelsesret- og praksis.

Der er ikke krav om, at en databeskyttelsesrådgiver skal have en bestemt uddannelsesmæssig baggrund, f.eks. som jurist.

Som udgangspunkt kan alle, VBC finder kvalificeret til at være databeskyttelsesrådgiver, varetage funktionen.

Følgende kan derfor være databeskyttelsesrådgivere:

- En intern medarbejder
- En fælles databeskyttelsesrådgiver for hele eller flere organisationer
- En ekstern databeskyttelsesrådgiver.

VBC kan vælge at benytte sig af en fælles databeskyttelsesrådgiver sammen med andre skoler, dog under den forudsætning, at det er i overensstemmelse med deres organisatoriske struktur og størrelse. I den forbindelse kan det være relevant at overveje, om databeskyttelsesrådgiveren skal fungere på baggrund af én ansættelseskontrakt for to forskellige myndigheder eller to deltidskontrakter.

Der er ikke et krav om fysisk tilstedeværelse på alle lokationer, såfremt VBC anvender en fælles databeskyttelsesrådgiver. Der er derfor mulighed for at aftale, hvordan den fysiske tilgængelighed i praksis kan løftes, herunder f.eks. ved hjælp af mail, telefon, internet m.m.

Databeskyttelsesrådgiverens opgaver

Databeskyttelsesrådgiveren funktion består i at rådgive den dataansvarlige og hjælpe med at VBC efterlever de databeskyttelsesretlige regler.

Databeskyttelsesrådgiveren skal inddrages i alle de overvejelser og vurderinger, som organisationen gør sig for at overholde kravene i databeskyttelsesforordningen, databeskyttelsesloven og øvrige regler for behandling af personoplysninger.

Databeskyttelsesrådgiveren skal endvidere som <u>minimum</u> varetage følgende opgaver:

1. Underrette og rådgive organisationen og de ansatte om databeskyttelse
2. Overvåge overholdelsen af de databeskyttelsesretlige regler i organisationen
3. Rådgivning i forbindelse med udarbejdelse af organisationens konsekvensanalyser
4. Samarbejde med Datatilsynet på vegne af organisationen
5. Være kontaktpunkt for tilsynsmyndigheden (Datatilsynet) angående alle spørgsmål om behandling af personoplysninger for de personer, der behandles oplysninger om

Ad. 1:

Det indebærer:

- Konkret rådgivning om beskyttelse af personoplysninger i organisationen samt overvejelser og beslutninger om, hvordan compliance sikres m.v., f.eks. i forbindelse med følgende:
    - Organisationens indkøb af nyt IT-system, kravsspecifikationer til leverandører,
    - Udarbejdelse af organisationens data-politikker,
    - Iværksættelse af behandling af personoplysninger,
    - Overvejelser om, hvorvidt en given behandling af personoplysninger overholder de generelle behandlingsregler
- Stå til rådighed for ansatte samt ledelsen i organisationen vedrørende spørgsmål om databeskyttelse,
- Rådgivning i forbindelse med udarbejdelse af organisationens konsekvensanalyser,
- Modtage underretning om og rådgive organisationen i forbindelse med brud på persondatasikkerheden

Ad. 2:

Det indebærer bl.a. at overvåge:

- Organisationens politikker om databeskyttelse
- Uddannelse af personale i databeskyttelse
- Oplysningskampagner
- Fordeling af ansvar
- Revisioner

Ad. 3:
I visse tilfælde skal VBC udarbejde en konsekvensanalyse af en planlagt behandling af personoplysninger. I de tilfælde skal VBCs databeskyttelsesrådgiver rådføres. Herudover skal databeskyttelsesrådgiveren rådgive med hensyn til udarbejdelse af konsekvensanalyse, når der anmodes herom.

Se endvidere skabelon for udarbejdelse af konsekvensanalyse (DPIA).

Ad. 4:

Databeskyttelsesrådgiveren skal samarbejde med tilsynsmyndigheden og fungere som tilsynsmyndighedens kontaktperson.

Ad. 5:

Databeskyttelsesrådgiveren skal inddrages i tilfælde af, at konkrete klagesager indbringes for Datatilsynet. Databeskyttelsesrådgiveren bør ligeledes orienteres, når Datatilsynet beslutter at gennemføre et eventuelt tilsyn af den dataansvarlige.

Herudover skal databeskyttelsesrådgiveren også være i stand til at vejlede den person, der behandles personoplysninger om. Det betyder, at databeskyttelsesrådgiveren skal være i stand til at vejlede om, hvilke rettigheder den pågældende har, og hvordan de kan udnyttes.

Det indebærer endvidere, at VBC skal give meddelelse om kontaktoplysninger på databeskyttelsesrådgiveren.

Der er intet til hinder for, at VBCs databeskyttelsesrådgiver varetager flere opgaver end de ovenforstående.

I databeskyttelsesrådgiverens funktionsbeskrivelse bør det klart defineres, hvilke opgaver, der påhviler databeskyttelsesrådgiveren

Kontrol og dokumentation

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

VBC dokumenterer

- At vi har en databeskyttelsesrådgiver, såfremt vi er forpligtet hertil
- At databeskyttelsesrådgiveren er uafhængig og ansat på baggrund af faglige kvalifikationer
- At databeskyttelsesrådgiveren inddrages i alle overvejelser og vurderinger i relation til behandling af personoplysninger
- At den løbende kontrol er udført

Bilag 10: Retningslinje om ansvarsfordeling (dataansvarlig/ 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 Vejen Business College (VBC), der behandler personoplysninger.

Formål

Formålet med denne retningslinje er at sikre, at VBC 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 VBC. Databeskyttelsesrådgiverens funktion er at understøtte, at VBC overholder reglerne i forordningen.

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 VBC 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 VBC 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 VBC 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 VBC, der er dataansvarlig, og altså ikke den enkelte ansatte.

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

Dataansvarliges forpligtelser

VBC 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 VBC 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 VBC 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 VBC 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 VBC. Vi skal sikre os, at databehandleren instrueres i, at denne altid skal underrette VBC 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 VBC har med vores databehandler.

Databehandler

Hvis VBC 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 VBC 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 bilag 4 ”Retningslinje om fortegnelse over behandlingsaktiviteter”.

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

Fælles dataansvarlige

I visse tilfælde kan VBC 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 VBC 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

Kontrol og dokumentation

VBC skal sikre, at der løbende foretages en dokumenteret kontrol af, at denne retningslinje efterleves.

VBC 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