**Databeskyttelsesrådgiverens evaluering af en behandlingsaktivitet**

|  |  |
| --- | --- |
| Organisation | **Databeskyttelsesrådgiverfunktion i Den Storkøbenhavnske Digitaliseringsforening (DSD)** |
| Dokument navn | DPO - Evaluering af behandlingsaktivitet v.1.0 docx |
| Dokument ejer | Daniel Soelberg Bach |
| Senest ændret | Juni 2019 |
| ISO 27002 |  |
| GDPR-reference | Art. 35.2.Den dataansvarlige rådfører sig med databeskyttelsesrådgiveren Art 38.1.Den dataansvarlige sikrer, at databeskyttelsesrådgiveren inddrages i alle spørgsmål vedrørende beskyttelse af personoplysninger |
| Dataklassifikation | Internt dokument |

Indhold

[Formål 1](#_Toc533024807)

[Metodebeskrivelse 1](#_Toc533024808)

[Generelle oplysninger 2](#_Toc533024809)

[Overordnet beskrivelse af behandlingsaktiviteten 2](#_Toc533024810)

[Behandlingshjemmel 4](#_Toc533024811)

[Registreredes rettigheder 5](#_Toc533024812)

[Privacy by design/default 5](#_Toc533024813)

[Leverandørforhold 5](#_Toc533024814)

[Behandlingsaktivitetens fortegnelse 6](#_Toc533024815)

[Risikovurdering 6](#_Toc533024816)

[Sikkerhedsforanstaltninger 7](#_Toc533024817)

[DPO evaluering 10](#_Toc533024818)

# Formål

DPO’en skal bistå den dataansvarlige med evaluering af en behandlingsaktivitets risikoniveau for de registrerede. Denne standardblanket afskildrer de essentielle elementer, som er nødvendige for DPO’ens evaluering af behandlingsaktivitetens risikoniveau (risiciene af varierende sandsynlighed og alvor) for beskyttelse af fysiske personers rettigheder.

# Metodebeskrivelse

Den dataansvarlige (herefter fagansvarlige), udfylder blanketten med henblik på at give et fyldestgørende billede af behandlingsaktiviteten og/eller en ny løsning, hvor der skal behandles personoplysninger.

Detaljeniveauet afstemmes under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder.

Den fagansvarlige sender den udfyldte blanket til DPO’en, som herefter evaluerer behandlingens lovlighed og risikoniveau for de registrerede. DPO’en kan, hvis nødvendigt, indhente yderligere oplysninger og detaljer for behandlingen.

I tilfælde af en type behandling, som navnlig ved brug af nye teknologier og i medfør af sin karakter, omfang, sammenhæng og formål, sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder, anmoder DPO ’en den fagansvarlige om, forud for iværksættelse af behandlingen, at analysere påtænkte behandlingsaktivitets konsekvenser for beskyttelse af personoplysninger jf. forordningens artikel 35.

Evalueringsprocessen afsluttes med DPO’ens udtalelse og eventuelle bemærkninger, observationer og/eller anbefalinger under hensyntagen til behandlingens lovlighed, formål, risikovurdering og foranstaltninger for beskyttelse af personoplysninger.

DPO’en returner blanketten til den fagansvarlige, som sikrer, at DPO ’ens udtalelse vedlægges den øvrige dokumentation for behandlingsaktiviteten med henblik på at kunne påvise tilstrækkeligt og rettidigt inddragelse af DPO’en vedrørende spørgsmål om beskyttelse af personoplysninger.

**Følgende udfyldes af fagansvarlig**

# Generelle oplysninger

Notér de generelle oplysninger om løsningen.

|  |  |
| --- | --- |
| **Udfyldt af** | NAVN + DATO |
| Fagansvarlige (dataansvarlige) | ANGIV NAVN |
| **Navn på løsningen**  *(kaldenavn på løsningen)* | ANGIV NAVN |
| **Formål med behandlingen**  *(beskrivelsen skal give et overblik over hvad løsningen skal anvendes til)* | BESKRIV FORMÅL |
| **Type af anskaffelse** | Ny løsning  Ændring af eksisterende løsning  Genforhandling af kontrakt  Andet: *angiv* |

# Overordnet beskrivelse af behandlingsaktiviteten

|  |  |  |
| --- | --- | --- |
| **Spørgsmål** | **Svar** | **Uddybende svar** |
| **Behandling af personoplysninger** | | |
| 1. Skal løsningen anvendes til personoplysninger jf. Databeskyttelsesforordningens artikel 6 | Ja  Nej | Hvis ja, angiv det potentielle antal af registrerede i behandlingen |
| 1. Skal der behandles følsomme personoplysninger i løsningen jf. Databeskyttelsesforordningens artikel 9? | Ja, angiv kategorier til højre  Nej | Angiv kategorier  Racemæssig eller etnisk oprindelse  Politisk overbevisning  Religiøs overbevisning  Filosofisk overbevisning  Fagforeningsmæssige forhold  Genetiske data  Biometriske data  Helbredsoplysninger, herunder misbrug af medicin, narkotika, alkohol m.v.  En fysisk persons seksuelle forhold eller seksuelle orientering  Hvis ja, angiv det potentielle antal af registrerede i behandlingen |
| 1. Skal der behandles oplysninger om straffedomme, Jf. Databeskyttelsesforordningens artikel 10 | Ja, angiv kategorier til højre  Nej | Angiv kategorier  Straffedomme  Lovovertrædelser  Hvis ja, angiv det potentielle antal af registrerede i behandlingen |
| 1. Skal der behandles oplysninger om cpr-nummerjf. Databeskyttelsesloven § 11 | Ja  Nej | Hvis ja, angiv det potentielle antal af registrerede i behandlingen |
| **Arkitektur overblik** | | |
| 1. Angiv det overordnede design | *Angiv ét eller flere udsagn* | webløsning til intern brug  webløsning til ekstern brug  webløsning både til intern og ekstern brug  Databaseløsning  Andet, indtast oplysning: |
| 1. Hvilken driftstype er aftalt? | *Angiv ét eller flere udsagn* | Driftes internt  Driftes internt med supportaftale  Hostes hos leverandør og evt. underleverandører |
| 1. Findes der et dataflow diagram der viser hvorledes personoplysningerne flyder fra indsamling til sletning? | Ja  Nej | Hvis ja, vedlæg diagram over dataflow |
| 1. Er der videregivelse af personoplysninger? | Ja  Nej | Hvis ja, hvilket hjemmel ligger til grund for videregivelsen. |
| 1. Modtagere af personoplysninger | Ja  Nej | Hvis ja, angiv kategorier af modtagere og geografisk lokalisering. |

# Behandlingshjemmel

|  |  |  |
| --- | --- | --- |
| **Spørgsmål** | **Svar** | **Uddybende svar** |
| **Almindelige personoplysninger (artikel 6) Udfyldes kun hvis der behandles almindelige personoplysninger** | | |
| 1. Er der hjemmel til behandlingen? | Ja, angiv kategorier til højre  Ikke hjemmel | Samtykke  Kontraktlig nødvendighed  Retlig forpligtigelse  Vital interesse  Opgave i samfundets interesse  Offentlig myndighedsudøvelse  Hvis retlig forpligtigelse eller offentlig myndighedsudøvelse angiv det bagvedliggende lovgrundlag: |
| **Følsomme personoplysninger (artikel 9) Udfyldes kun hvis der behandles følsomme personoplysninger** | | |
| 1. Er der hjemmel til behandlingen? | Ja, angiv kategorier til højre  Ikke hjemmel | Samtykke  Vital interesse  Offentliggjort af registrerede  Fastlæggelse af retskrav  Arbejds-, sundheds- og social retlige forpligtigelser + rettigheder  Væsentlig samfundsinteresse  Forebyggende medicin eller arbejdsmedicin  Samfundsinteresser på folkesundhedsområdet  Hvis afkrydsning i et eller flere af de ovenfor anførte fem felter angiv bagvedliggende lovgrundlag: |
| **Betingelser for samtykke (artikel 7) Udfyldes kun hvis samtykke er hjemmel** | | |
| 1. Indhentes et specifik, informeret og utvetydigt samtykke, der kan påvises? | Ja  Nej | *Hvis ja, angiv eksempelvis procedure, politikker eller andet bilag der kan påvise samtykket.* |
| 1. Oplyses der om, forinden der givers samtykke, at samtykket til enhver tid kan trækkes tilbage? | Ja  Nej |  |
| 1. Er der skriftlige procedurer for tilbagetrækning af samtykke? | Ja  Nej |  |

# Registreredes rettigheder

|  |  |  |
| --- | --- | --- |
| **Spørgsmål** | **Svar** | **Uddybende svar** |
| **Oplysningspligt (artikel 13 og artikel 14)** | | |
| 1. Er oplysningspligten opfyldt ved indsamling af oplysninger hos den registrerede eller via tredjemand? | Ja  Nej | Hvis ja, beskriv hvordan |

# Privacy by design/default

|  |  |  |
| --- | --- | --- |
| **Spørgsmål** | **Svar** | **Uddybende svar** |
| **Databeskyttelse gennem design og standardindstillinger (artikel 25)** | | |
| 1. Er sikring af databeskyttelse gennem design etableret? | Ja  Nej | Hvis ja, *beskriv eksempelvis: Applikationen har roller med adgangsbegrænsning jf. fagligt behov. Pseudonymisering og dataminimering mv. etableret?* |
| 1. Er sikring af databeskyttelse gennem standardindstillinger etableret? | Ja  Nej | Hvis ja, *beskriv eksempelvis: Applikationen har standardindstillinger der begrænser eksponering af de registreredes personoplysninger.* |
| 1. Tillader behandlingen minimering af personoplysninger i systemet? | *Angiv ét udsagn* | Løsningen behandler kun de nødvendige personoplysninger der er brug for (dataminimering)  *Beskriv, eksempelvis: indtastningsfelter giver ikke mulighed for at indtaste fritekst* |

# Leverandørforhold

|  |  |  |
| --- | --- | --- |
| **Spørgsmål** | **Svar** | **Uddybende svar** |
| **Databehandler – behandling af personoplysninger på vegne af den dataansvarlige (artikel 28 og artikel 29)** | | |
| 1. Gøres der brug af databehandler i denne behandling? | Ja  Nej | Kun ved ja til dette spørgsmål udfyldes de nedenstående spørgsmål. |
| 1. Findes der en gyldig kontrakt? | Ja  Nej | Hvis ja, angiv ... |
| 1. Findes der en gyldig databehandleraftale? | Ja  Nej | Hvis ja, angiv bilag |
| 1. Har databehandleren nogle anerkendte branchecertificeringer? | Ja  Nej | Hvis ja, angiv hvilke |
| 1. Leverer databehandleren uvildige revisionserklæringer? | Ja  Nej | Hvis ja, angiv erklæringstyper (f.eks. ISAE 3000 type II) og vedlæg disse i besvarelsen. |
| 1. Har databehandleren foretaget en selvstændig risikovurdering af behandlingen af personoplysninger? | Ja  Nej |  |
| 1. Hvis ja, udleverer databehandleren risikovurdering af løsningen? | Ja  Nej | Hvis ja, vedlæg besvarelsen. |
| 1. Har Databehandler etableret passende tekniske og organisatoriske sikringsforanstaltninger for at sikre et passende sikkerhedsniveau (afpasset med dataansvarliges risikovurdering)? | Ja  Nej | Hvis ja, angiv bilag for tekniske og organisatoriske foranstaltninger. |
| 1. Er fysiske personer hos databehandleren og underdatabehandlere instrueret i håndtering af personoplysninger i henhold til den dataansvarliges instruks. | Ja  Nej |  |
| 1. Her databehandleren en beskrivelse af anvendelsen af underdatabehandlere, herunder beskrivelse af underdatabehandlernes tekniske og organisatoriske foranstaltninger til beskyttelse af den registreredes rettigheder og behandlingen af personoplysninger? | Ja  Nej |  |
| 1. Har databehandler personale eller underleverandører uden for DK? | Ja  Nej | Hvis ja, hvor befinder de sig geografisk? |
| 1. Har databehandler modtaget instruks for behandling og beskyttelse af personoplysninger fra den dataansvarlige? | Ja  Nej |  |
| 1. Foreligger der skriftlige procedurer, som beskriver, at databehandler alene må behandle personoplysninger, herunder overførsel af personoplysninger til et tredjeland eller en international organisation, efter dokumenteret instruks fra den dataansvarlige eller i henhold til EU-ret eller national ret? | Ja  Nej |  |

# Behandlingsaktivitetens fortegnelse

|  |  |  |
| --- | --- | --- |
| **Emne** | **Verificér** | **Kontroller** |
| **Fortegnelse over behandlingsaktiviteter (artikel 30)** | | |
| 1. Foreligger der en fortegnelse for behandlingsaktiviteten? | Ja  Nej | Hvis ja, vedlæg dokument eller link til fortegnelsen. |

# Risikovurdering

|  |  |  |
| --- | --- | --- |
| **Spørgsmål** | **Svar** | **Uddybende svar** |
| **Risikovurdering (artikel 32)** | | |
| 1. Er der foretaget en risikovurdering af behandlingen? | Ja  Nej | Hvis ja, angiv datoen for risikovurderingen og eventuelle bilag. |
| 1. Hvis det drejer sig om fornyelse af en behandlingsaktivitet, har risikobilledet ændret sig siden sidste risikovurdering | Ja  Nej | Hvis ja, angiv hvilke elementer der har ændret sig |
| 1. Udviser risikovurderingen en sandsynlig høj risiko for de registrerede? | Ja  Nej |  |
| **Konsekvensanalyse vedrørende databeskyttelse (artikel 35) Udfyldes kun hvis der er sandsynlig høj risiko for de registrerede** | | |
| 1. Er der udarbejdet en konsekvensanalyse (DPIA)? |  | Hvis ja, angiv datoen for analysen og eventuelle bilag. |

# Sikkerhedsforanstaltninger

Angiv hvilke sikkerhedsforanstaltninger der er etableret.

|  |  |  |
| --- | --- | --- |
| **Emne** | **Verificér** | **Kontroller** |
| **Den dataansvarliges ansvar – implementering af passende databeskyttelse (artikel 24 og 32)** | | |
| 1. **Brugere af løsningen** | *Angiv ét eller flere udsagn* | Medarbejdere  Borgere  Samarbejdspartnere  Andre Angiv hvem |
| 1. **Brugerstyring**   *Hvem styrer oprettelse af brugere?* | *Angiv ét eller flere udsagn* | Af Kommunens sikkerhedsadministratorer  Af It-funktionen  Af Leverandøren  AndreKlik her for at angive tekst. |
| *Hvordan lukkes brugere?* | Af Kommunens sikkerhedsadministratorer  Af It-funktionen  Af Leverandøren  AndreKlik her for at angive tekst. |
| 1. **Adgangsrettigheder** | | |
| *Tildeles brugeren kun adgangsrettigheder til at tilgå personoplysninger, som brugeren har arbejdsmæssigt behov for?* | Ja  Nej | Hvis ja, beskriv hvordan? |
| 1. **Login, intern** | *Angiv ét eller flere udsagn* | Personligt brugernavn og kodeord  ADFS  Multifaktor  Blokering ved for mange afviste adgangsforsøg  Brugere kan låse egen konto op via selvbetjeningsløsning |
| 1. **Login, ekstern** | *Angiv ét eller flere udsagn* | Personligt brugernavn og kodeord  ADFS  Multifaktor  Nemid  Blokering ved for mange afviste adgangsforsøg  Brugere kan låse egen konto op via selvbetjeningsløsning |
| 1. **Hvordan styres brugere med privilegerede rettigheder** | *Angiv ét eller flere udsagn* | Brugernavn kun til admin formål  Krav om multifaktor når adminrettigheder ønskes anvendt  Som almindelige brugere  Fælles brugernavn og password |
| 1. **Udskiftning af brugerpassword** | *Angiv udsagn* | Password udskiftes aldrig  Password udskiftes hver 3. måned  Password udskiftes ikke, der anvendes multifaktor hos alle brugere |
| 1. **Hvor opbevares data?** | *Angiv ét eller flere udsagn* | Database  Server  Fildrev  Hos leverandør på navngiven fysisk lokation  Hos leverandør i en cloudløsning  Andet Klik her for at angive tekst. |
| 1. **Beskyttelse af data i løsningen**   *Hvordan bliver data beskyttet på databaser, på servere og evt. fildrev* | *Angiv ét eller flere udsagn* | Pseudonymisering  Kryptering  Gennem begrænset adgang  Alarmer når der foretages ændringer i systemet  Adgangsstyring  Ingen  Andet Klik her for at angive tekst. |
| 1. **Arbejdsstationer** | | |
| Stationær pc | *Angiv ét eller flere udsagn* | Brugernavn + password  Kryptering  Styring via MDM løsning eller lignende  Multifaktor autentifikation: Klik her for at angive tekst.  Tyverisikring |
| Bærbar pc | Brugernavn + password  Kryptering  Styring via MDM løsning eller lignende  Multifaktor autentifiation: Angiv metode  Tyverisikring  Tracking/wiping i tilfælde af tyveri |
| Håndholdte enheder (smartphones, tablets mfl.) | Brugernavn + password  Kryptering  Styring via MDM løsning eller lignende  Multifaktor autentifikation: Angiv hvordan  Tyverisikring  Tracking/wiping i tilfælde af tyveri |
| 1. **Datatransmission**   *Angiv hvordan data transmitteres til brugere uden for Kommunen.* | *Angiv ét eller flere udsagn* | Krypteret ANGIV TYPE  MPLS eller lignende  VPN  Anden sikker løsning Klik her for at angive tekst.  Ikke relevant |
| 1. **Overvågning**   *Hvordan bliver løsningen overvåget?* | *Angiv ét eller flere udsagn* | Løsningen overvåges af Kommunens It-funktion  Løsningen overvåges af leverandør  Overvågning sker aktivt og forsøg på misbrug registreres og håndteres  Kapaciteten overvåges og der foretages optimering proaktivt  Ikke relevant angiv årsag |
| 1. **Support** | *Angiv ét eller flere udsagn* | It-funktionen i Kommunen står for support af løsningen  Leverandøren står for support af løsningen |
| 1. **Ændringer** | *Angiv ét eller flere udsagn* | Ændringer sker i henhold til ændringsstyringsprocedurer  Ændringer sker ad hoc  Ændringer godkendes af bemyndiget person i kommunen inden de iværksættes |
| 1. **Udvikling og test**   Hvordan sker udvikling af ændringer og test af disse? | *Angiv udsagn* | Udvikling og test foregår i adskilt miljø fra driftsløsningen  Udvikling og test foregår i driftsmiljøet |
| 1. **Logning**   *Er det muligt at trække en maskinlæsbar log som kan overføres til kommunens logningsløsning? Filen skal indeholde: CPR på den borger der søges på, tidsstempel, beskrivelse af søgekriterie, den medarbejder der har søgt* | *Angiv udsagn* | Ja  Nej angiv årsag |
| 1. **Sikring mod cyberangreb**   *Hvilke sikkerhedsforanstaltninger er implementeret?* | *Angiv ét eller flere udsagn* | Beskyttelse mod DDoS angreb  Sikring mod hackerangreb  Sikring mod phishing  Malware og virus  Positivliste/negativliste over godkendte programmer i løsningen  Opdatering af højrisiko-sikkerhedsopdateringer installeres inden for 2 dage  Antallet af brugere med privilegerede rettigheder er på et absolut minimum  Foretages der jævnlige penetrationstest af løsningen og følges der op på dem? |
| 1. **Backup og restore**   Hvordan er backup-løsningen? | *Angiv ét eller flere udsagn* | Backup foretages af It-funktionen  Backup foretages af leverandør  Back up sker i henhold til aftalt backup vejledning  Backupmedier opbevares på et site adskilt fra driftsmiljøet  Test af backup sker angiv frekvens  Der er udarbejdet planer og dokumentation for restore af løsningen  Disaster recovery test udføres angiv frekvens |
| 1. **Beredskab**   Er der etableret nødplaner og beredskabsplaner i tilfælde af nedbrud? | *Angiv ét eller flere udsagn* | Forvaltningerne er ansvarlige for nødplaner  It-funktionen er ansvarlig for etablering af nøddrift i tilfælde af katastrofer ol. |
| 1. **Politikker og procedurer** | | |
| Er der etableret politikker og procedurer som sikrer, at behandlingen lever op til behandlingsregler, behandlingsprincipper og behandlingssikkerhed. | Ja  Nej | Hvis ja, angiv bilag |
| 1. **Eventuelle andre foranstaltninger** | Ja  Nej | Hvis ja, angiv hvilke |

**Følgende udfyldes af DPO’en**

# DPO evaluering

Udfyldes af DPO

Materiale der ligger til grund for evalueringen af behandlingen:

|  |
| --- |
| Navn på bilag |
|  |
|  |
|  |
|  |

**Bemærkninger**

Under hensyntagen til skemaets oplysninger og tilhørende bilag, attesterer DPO’en med følgende bemærkninger:

|  |  |  |
| --- | --- | --- |
| **Observation** | **Vurdering** | **Anbefaling** |
|  |  |  |
|  |  |  |
|  |  |  |