**Mal: Vurdering av personvernkonsekvenser (DPIA)**

|  |
| --- |
| Navn på system/prosjekt:  Blockchain for transparent rekruttering - Et system for å verifisere arbeidserfaring |
| DPIA-en utføres av:  Kandidat 4 – Høgskolen i Molde Bachelor vår 2025 |
| Dato:  4.april 2025 |

**1. Systematisk beskrivelse av behandlingen**

I denne fasen er målet at den behandlingsansvarlige skal ha en fullstendig oversikt over behandlingen, og sørge for at beskrivelsene som er gjort er komplette og tydelige.

1. Overordnet oversikt

|  |
| --- |
| Prosjektet skal gi brukere mulighet til å registrere, lagre og eventuelt dele sin arbeidshistorikk digitalt. Dette skal gi brukeren eierskap til egen kompetansedokumentasjon og legge til rette for tillitsbasert deling av CV-lignende informasjon. Systemet bruker både sentral database (med slettemulighet) og valgfri offentlig blockchain (Ethereum) for lagring og som kan verifiseres av arbeidsgiver.  Prosjektet har høy personvernrisiko knyttet til blockchain, men gjennom klare tekniske og organisatoriske tiltak, særlig ved å tilby en trygg database-løsning og frivillig on-chain lagring, kan risikoen reduseres til akseptabelt nivå. |

1. **Behandlingens art**

Behandlingens iboende karakteristikk og hvordan behandlingsaktivitetene skal foregå. Beskrivelser av hva dere planlegger å gjøre med personopplysningene.

|  |  |
| --- | --- |
| Hvordan skal personopplysningene samles inn? | *Registrerte brukere* |
| Hvordan skal personopplysningene lagres? | *Database (MongoDB)* |
| Hvordan skal personopplysningene brukes? | *Identifisering ved innlogging/brukerdata* |
| Hvem skal ha tilgang til personopplysningene? | *Ansvarlig for database* |
| Hvem skal det samles inn personopplysninger om? | *Arbeidssøkere og arbeidsgivere* |
| Hvordan kan den registrerte utøve sine rettigheter? | *Sletting av profil/data. Nedlasting av data som CSV* |
| Vil det være systematisk behandling av personopplysninger? | *Ja* |
| Brukes det ny teknologi eller ny bruk av eksisterende teknologi hvor personvernkonsekvenser ikke har blitt vurdert? | *Ja Offentlig tilgjengelighet av opplysninger* |

1. **Behandlingens omfang**

|  |  |
| --- | --- |
| Kategorier av personopplysninger som behandles | *Nei. GDPR artikkel 9.* |
| Antall registrerte involvert i behandlingen | *…* |
| Datavolum | *Uvisst – (moderat)* |
| Behandlingsfrekvens | *Hver gang brukeren velger å registrere ny arbeidshistorikk.* |
| Lagringstid for personopplysningene | *Kort til permanent* |
| Geografisk omfang | *Lokalt men kan nå globalt* |

1. **Behandlingens formål**

|  |  |
| --- | --- |
| Behandlingens formål | *La enkeltpersoner selv registrere og dokumentere sin arbeidshistorikk på en uforanderlig og offentlig tilgjengelig blockchain.*  *Styrke eierskap og kontroll over egen CV-data, uten behov for sentrale aktører.*  *Gjøre opplysningene sporbare og transparente, og muliggjøre tredjepartsverifikasjon utenfor kontrakten.* |
| Vil det være kontrollformål? | *Nei* |
| Er formålet å treffe avgjørelser om enkeltpersoner basert på systematisk og omfattende analyse av personlige aspekter? | *Nei* |
| Har behandlingen av personopplysninger som mål å ta beslutninger som får betydning for den registrerte? | *Nei* |
| Skal opplysningene brukes til å profilere den registrerte? | *Nei* |
| Brukes personopplysninger for å avdekke ukjente sider eller for å gjenkjenne mønstre ved den registrerte? | *Nei* |
| Vil personopplysningene viderebehandles til nye eller andre formål? | *Nei* |

1. **Sammenhengen behandlingen utføres i (kontekst)**

Her er målet å se behandlingen i et større bilde og vurdere alle interne og eksterne faktorer som kan påvirke forventninger eller konsekvenser.

|  |  |
| --- | --- |
| Hvilke kilder brukes for innhenting av personopplysninger? | *Brukeren selv* |
| Relasjon mellom behandlingsansvarlig og den registrerte | *Brukeren er både registrert og den som initierer behandlingen; desentralisert modell uten klassisk behandlingsansvarlig.* |
| I hvilken grad har den registrerte kontroll over sine opplysninger? | *Full kontroll ved innlegging av data, sletting av data database – ingen sletting etter opplasting til blockchain* |
| Beskriv hvordan behandlingen vil oppfattes fra den registrertes synsvinkel | *Som en trygg måte å dokumentere arbeidshistorikk, men også potensielt risikabelt grunnet offentlig og permanent lagring.* |
| Vil den registrerte ha en særskilt forventning om konfidensialitet? | *Ja, mange kan forvente at arbeidshistorikk behandles fortrolig – noe som ikke er tilfelle her.* |
| Vil den registrerte ha en særskilt forventning om at personopplysningene er nødvendige og korrekte? | *Ja, spesielt dersom data brukes i jobbsøker- eller verifiseringsøyemed.* |
| Vil den registrerte ha en særskilt forventning om privatliv? | *Ja og nei, siden arbeidserfaring ofte oppleves som personlig informasjon.* |
| Vil det behandles personopplysninger om barn, pasienter eller andre kategorier av personer som defineres som sårbare? | *Ikke planlagt, men ikke teknisk forhindret. Risikoen finnes.* |
| Finnes det tidligere erfaring med tilsvarende type behandling? | *Begrenset erfaring; bruk av blockchain for personopplysninger er fortsatt nytt og lite regulert* |
| Beskriv eventuelle relevante fremskritt innen teknologi eller sikkerhet | *Fremskritt innen zero-knowledge proofs, off-chain lagring og desentralisert identitet (DID) kan redusere risiko på sikt. (*[*https://chain.link/education/zero-knowledge-proof-zkp*](https://chain.link/education/zero-knowledge-proof-zkp)*)* |
| Finnes det noen nåværende tilfeller av allmenn bekymring for den beskrevne måten å behandle personopplysninger på? | *Ja. Det er utbredt bekymring i fagmiljøer og tilsyn for uforanderlig lagring av persondata på blockchain uten slettemulighet.* |
| Vil dere behandle personopplysninger fra ulike datasett, som er innsamlet for ulike formål og fra ulike behandlingsansvarlige? | *Nei. All informasjon legges inn frivillig av brukeren selv. Det hentes ikke data fra eksterne kilder, registre eller behandlingsansvarlige.* |
| Kobles ulike registre for å gi ny type informasjon om den registrerte? | *Nei (ikke i selve systemet). Men det finnes en potensiell risiko for at tredjeparter (utenfor systemet) kan koble offentlig blockchain-data med andre åpne eller kommersielle datasett for å profilere brukere.* |

1. **Identifisering og oversikt**

|  |  |
| --- | --- |
| Behandlingsansvarlig: | *Kandidatnr: 4* |
| Felles behandlingsansvarlig: | *Nei* |
| Databehandler(e): | *Nei* |

1. **Mottakere av personopplysninger**

|  |  |
| --- | --- |
| Beskriv alle mottakere/kategorier av mottakere av personopplysninger | *Offentlig tilgjengelig på blockchain – alle med tilgang til nettverket er potensielle mottakere.* |
| Hvordan deles personopplysningene mellom avdelinger **internt** i virksomheten? | *Ikke aktuelt – ingen intern deling, da systemet er desentralisert.* |
| Hvilke **eksterne** virksomheter deles personopplysningene med? Hvis ja, for hvilke formål og med hvilke rettslige grunnlag? | *Ingen aktiv deling* |
| Overføres personopplysningene til land utenfor EU/EØS-området (tredjestater), jf. art. 44-49? Hvis ja, hva er det rettslige grunnlaget for det? | *Ja, indirekte. Data publiseres globalt på Ethereum-nettverket. Ingen jurisdiksjon over hvem som får tilgang.* |
| Beskriv hvilke forholdsregler som tas for å beskytte personopplysninger | *Brukerveiledning, dataminimering, frivillig innlegging, kryptering database* |
| Er alle databehandlere identifisert, og er forholdet til dem avklart gjennom avtaler, jf. art. 28 nr. 3? | *Ikke aktuelt.* |
| Gir databehandleren tilstrekkelige garantier for at egnede tekniske og organisatoriske tiltak som sikrer at behandlingen er i samsvar med forordningen, vil gjennomføres? | *Ikke aktuelt. Ingen databehandler, og ingen ansvarlig behandlingsinstans* |

1. **Dataflyt, lagring og mellomlagring**

|  |  |
| --- | --- |
| Hvordan overføres og tilgjengeliggjøres personopplysningene? | *Data legges inn av brukeren via en smartkontrakt og lagres offentlig og uforanderlig på Ethereum-blockchain, tilgjengelig for alle med nettverkstilgang.* |
| Hvor og hvor lenge lagres personopplysningene ulike steder? | *Lagres permanent på Ethereum-nettverket. Data lagret i database kan slettes når som helst av bruker* |
| Hvor lenge lagres personopplysningene etter at formålet ved behandlingen er over, før de slettes? Når skal opplysningene slettes? Er det utarbeidet sletterutiner? | *Blockchain tillater ikke fjerning av data Data i databasen slettes enkelt fra brukerens side i frontend.* |
| Er personopplysningssikkerheten tilstrekkelig ivaretatt? | *Delvis. Transaksjoner er sikre og kryptografisk beskyttet, men data er offentlig synlig og kan ikke skjules, slettes eller krypteres etter innlegging.*  *Ingen tilgangskontroll eller konfidensialitet utenom brukersiden – kun integritet og sporbarhet er ivaretatt.* |

1. **Informasjonssikkerhet**

|  |  |
| --- | --- |
| Gjennomgå den funksjonelle beskrivelsen av alle behandlinger og om alle aktiva som skal brukes er identifisert | *Brukere legger inn arbeidshistorikk (stilling, firma, år, beskrivelse) via smartkontrakt. Data knyttes til brukerens blockchain-adresse og lagres permanent.* |
| Tas ny teknologi i bruk, eller brukes eksisterende teknologi på en ny måte? | *Ja. Det brukes eksisterende blockchain-teknologi (Ethereum) på en delvis ny måte – til opplysningslagring, noe som ikke er uvanlig praksis men som innebærer nye risikoer.* |
| Har virksomheten bygget systemet fra grunnen av eller er det kjøpt ferdig (som hyllevare)) fra ekstern leverandør og deretter installert hos dere? | *Bygget fra grunnen av* |
| Er programvaren utviklet med innebygd personvern og personvern som standardinnstilling? | *Delvis. Systemet begrenser mulighet for opplasting. Personvern som standard er ikke fullt ut implementert pga. blockchainens uforanderlige og åpne natur.* |

Forsikre deg om at alle aktuelle referanser som er relatert til og aktuelle for behandlingen er dokumentert. Kan omfatte eksterne og interne krav, policy mv. som er nødvendige eller som må etterleves, f.eks.:

* Godkjente atferdsnormer/bransjenormer (art. 40)
* Sertifiseringer relatert til personvern (art. 42)
* Forskrifter, rundskriv, mv.

**2. Nødvendighet og proporsjonalitet**

I denne fasen kvalitetssikres det at valgene oppfyller personvernprinsippene, dvs. at de er legitimert og utført for å bidra til at behandlingen er nødvendig. For å etterleve lovkravene, må man også sjekke at valgene står i et rimelig forhold til formålene.

2.1 Personvernprinsippene

2.1.1 Rettslig grunnlag

|  |  |
| --- | --- |
| Rettslig grunnlag/behandlingsgrunnlag: | *Systemet forutsetter at brukeren selv legger inn opplysninger frivillig, hvilket impliserer samtykke (art. 6 nr.1a «GDPR»).* |
| Kommer det rettslige grunnlaget/behandlingsgrunnlaget tydelig frem for de registrerte? | *Delvis. Men det bør tydeliggjøres ved en brukerveiledning eller informasjonsside, slik at den registrerte forstår konsekvensene fullt ut.* |
| Omfatter rettslig grunnlag både egne formål og eventuell utlevering? | *Nei* |
| Vurder hvordan åpenhet ivaretas i behandlingen | *Begrenset. Selve smartkontrakten er åpen kildekode og transparent, og all data er synlig på blockchain. Men for registrerte brukere er det viktig å:*  *Forklare at data ikke kan slettes*  *Informere om offentlig tilgjengelighet*  *Tydeliggjøre hva slags data som bør/ikke bør legges inn* |

2.1.2 Formålsbegrensning

Formål(ene) skal være spesifikt, uttrykkelig angitt og berettiget, jf. art. 5 nr. 1 bokstav b.

|  |  |
| --- | --- |
| Er formålet klart definert? Er formålet definert slik at det samsvarer med forventningene til den registrerte? | *Ja. Formålet er å gi brukere mulighet til å dokumentere og lagre arbeidshistorikk permanent på blockchain. Dette er tydelig definert på nettstedet.* |
| Vurder om formålet kan oppnås med en mindre inngripende behandling | *Nei. Data må være offentlige og uforanderlige via blockchain for å oppnå desentralisering.* |
| Vurder hvorvidt formålet kan oppnås med anonyme eller pseudonyme alternativer | *Det er satt opp med database og blockchain for verifisering. Ser ingen andre alternativer.* |

2.1.3 Dataminimering

Personopplysninger skal være adekvate, relevante og begrenset til det som er nødvendig for formålene, jf. art. 5 nr. 1 bokstav c.

|  |  |
| --- | --- |
| Vurder om formålet kan oppnås med mindre datainnhenting | *Nei. Datainnsamlingen slik den står nå er minimal.* |
| Begrunn nødvendighet og relevans relatert til formål for hver enkelt variabel i et datasett | *Jobbtittel:* ***Nødvendig*** *– sentral del av arbeidserfaring*  *Firma:* ***Nødvendig****, men potensielt identifiserende*  *Ansettelsesperiode:* ***Nødvendig*** *– gir kontekst og kronologi*  *Rollebeskrivelse:* ***Delvis nødvendig*** *– gir ekstra innsikt, men bør være begrenset* |

2.1.4 Riktighet

Personopplysninger skal være korrekte og oppdaterte, jf. art. 5 nr. 1 bokstav d.

|  |  |
| --- | --- |
| Vurder hvordan personopplysninger holdes korrekte og oppdaterte, med og uten den registrertes involvering | *Ved brukerens involvering.* |
| Vurder om dere har nødvendig funksjonalitet for å rette og slette uriktige opplysninger | *Delvis. Data i databasen kan endres/slettes. Data lastet til blockchain blir liggende.* |
| Ut ifra den registrertes perspektiv, er det behov for kontradiksjon? | *Ja. Skrivefeil e.l. bør kunne elimineres.* |

2.1.5 Lagringsbegrensning

Personopplysninger skal slettes eller anonymiseres når formålet er oppnådd, jf. art. 5 nr. 1 bokstav e.

|  |  |
| --- | --- |
| Vurder om personopplysninger lagres etter at formålet er oppnådd | *Nei. Personopplysninger kan slettes når som helst fra frontend av bruker. Personopplysninger skal ikke lastes til blockchain* |
| Vurder hvilke garantier som må være på plass dersom personopplysninger skal lagres i lenge perioder grunnet arkivformål i allmennhetens interesse, for formål knyttet til vitenskapelig eller historisk forskning eller for statistiske formål, jf. art. 89 nr. 1. | *Data begrenses til det nødvendige* |

2.2 De registrertes rettigheter

|  |  |
| --- | --- |
| Vurder hvordan informasjon til de registrerte gis | *Det bør for eksempel. etableres en personvernerklæring der formål, risiko, lagringspraksis og rettigheter forklares tydelig. Dette er avgjørende for å overholde krav i art. 12 og 13 i «GDPR»* |
| Vurder innhenting av samtykke, jf. art 7 og 8 | *For at samtykke skal være gyldig må det være informert, frivillig, spesifikt og dokumenterbart, noe det ikke er.* |
| Vurder hvordan den registrertes rett til innsyn og til dataportabilitet ivaretas, jf. art. 15 og 20 | *Ivaretatt gjennom MongoDB (CSV)* |
| Vurder hvordan den registrertes rett til korrigering og sletting ivaretas, jf. 16 og 17 | *Delvis ivaretatt. Kan slette data i databasen. Blockchain er uforanderlig.* |
| Vurder hvordan den registrertes rett til innsigelser og begrensning av behandling ivaretas, jf. art. 18, 19 og 21 | *Kan slette egen bruker fra frontend.* |
| Vurder hvordan forbud mot automatiserte individuelle avgjørelser, herunder profilering, håndheves, jf. art. 22 | *Ikke teknisk mulig.* |

**3. Vurdering av risiko for de registrertes rettigheter og friheter, og planlagte tiltak for å**    
**håndtere risikoene**

I denne fasen skal man gjennomføre en vurdering av personvernkonsekvenser for den registrertes friheter og rettigheter etter forordningen. Først litt generelt om hva som skal gjøres her, så følger malen under.

3.1 Medbestemmelse, åpenhet og forutsigbarhet

Gjør en vurdering av risikoens opprinnelse, art, særegenhet og alvorlighetsgrad. Mer spesifikt bør det gjøres en vurdering ut ifra de registrertes perspektiv for hver risiko:

1. **Manglende reell medbestemmelse** – den registrerte har ikke et valg, får ikke informasjon, får ikke innsyn, osv.
2. **Manglende reell åpenhet** – virksomheten evner ikke å forklare komplekse behandlinger eller forventet resultat ved sammenstilling av personopplysninger med andre datasett osv.
3. **Manglende forutsigbarhet** ved behandlingen – behandlingen er utenfor det den registrerte vil forvente osv.

Her skal man også avklare potensielle **konsekvenser** for den registrertes personopplysningsvern for hvert risikoscenario. Hvilke konkrete rettigheter og friheter står i fare for å ikke innfris?

Eksempler på konsekvenser: Den registrerte har ikke mulighet til å utøve sine rettigheter, får ikke tilgang til tjenester eller muligheter, har manglende kontroll over bruken av personopplysninger, utsettes for diskriminering, utsettes for id-tyveri, svindel, økonomiske tap, tap av omdømme, fysisk skade, tap av konfidensialitet, reidentifisering av pseudonymiserte data, annen betydelig økonomisk eller sosial ulempe.

* Anslå **alvorlighetsgrad** for hver risiko, særlig avhengig av hvilken inngripen en potensiell virkning har på den registrerte.
* Identifiser **trusler** som kan føre til hendelser og hvilke risikokilder som kan forårsake dem.
* Anslå **sannsynlighet** for at en hendelse oppstår, særlig ut fra en sårbarhetsvurdering og hva slags evne en risikokilde kan ha for å utnytte dem.

3.2 Tiltak

Velg tiltak for å håndtere risikoene for de registrertes og andre berørte personers rettigheter og berettigede interesser. Identifiser eller bestem hva slags tiltak (garantier, sikkerhetstiltak og mekanismer) som kan håndtere risikoene. Slike tiltak kan typisk være:

* Spesifikke garantier for å minimere inngripen:
* Krav om fornyet samtykke
* Rett til reservasjon
* Innhenting av registrertes/representanters syn på behandlingen
* Forsterket informasjonsplikt (løpende informasjon, informasjon i flere kanaler, spesifikk informasjon om kobling mellom datasett og resultat av kobling osv.)
* Særskilt tilrettelagt innsynsportal
* Særskilte dataminimeringstiltak (monitorering bare i bestemte tidsrom eller spesifikke områder, øyeblikksbilder i stedet for kontinuerlig monitorering, avstå fra behandling av spesifikke opplysninger osv.)
* Tilrettelegging for dataportabilitet
* Automatisk sletting eller anonymisering ved kortere intervall enn lovkrav
* Hindre kobling mellom datasett
* Spesifikke sikkerhetstiltak som angår personopplysninger som skal behandles:
* Kryptering
* Anonymisering
* Partisjonering
* Tilgangskontroll
* Sporbarhet
* Generelle sikkerhetstiltak som iverksettes på systemet hvor behandlingen utføres:
* Operativ sikkerhet
* Back-up
* Sikkerhet på hardware
* Teknisk og fysisk styring
* Organisatoriske tiltak:
* Policy
* Rutiner
* Prosjektledelse
* Personellhåndtering og opplæring
* Håndtering av hendelser og brudd
* Forhold til tredjeparter

Identifiser og vurder risikoer:

|  |  |  |  |
| --- | --- | --- | --- |
| **Beskriv risikoen behandlingen har for de registrertes rettigheter og friheter, og hvilke konsekvenser den har for de registrerte** | **Alvorlighetsgrad for risikoen** | **Identifiser trusler som kan føre til hendelser** | **Sannsynlighet for at en hendelse oppstår** |
| |  | | --- | | Tap av kontroll over egne data |  |  | | --- | |  | | Uautorisert innsikt og profilering (fra database) |   Bruk av data i diskriminerende eller skadelige sammenhenger  Brudd på forventning om konfidensialitet og privatliv  Ugyldig samtykke / manglende informert valg | Kanslettes av brukeren selv via databasen  Begrenset – database krever innlogging, ikke offentlig  Kan begrenses siden brukeren selv styrer hva som deles, og data er ikke automatisk offentlig  Mye bedre kontroll i databasen enn ved blockchain-lagring  Hvis samtykke er informert og interaktiv, lav risiko | Minimal  Minimal  Betydelig  Minimal til betydelig  Minimal | Liten  Liten  Mulig  Liten til mulig  Liten |

Identifiser risikoreduserende og skadebegrensende tiltak:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Risiko** | **Tiltak** | **Effekt** **på** **risiko** | **Restrisiko** | **Tiltak** **godkjent** |
| Tap av kontroll over egne data  Manglende rett til sletting på blockchain  Manglende innsyn og dataportabilitet  Manglende tilgangskontroll i database  Profilering eller kobling av data på blockchain  Feilaktig eller uriktig informasjon | Bruker kan slette data fra database selv  Informasjon og advarsler før innlegging, kun nødvendige data lagres on-chain  Bruker kan laste ned profil og arbeidshistorikk som CSV  Tilgangsstyring, autentisering og logging implementert  Minimere informasjon som legges on-chain, pseudonymisering, off-chain bruk av sensitive felt  Bruker kan redigere/slette informasjon lastet ned som CSV | Reduserer risiko vesentlig  Reduserer alvorlighetsgrad  Risiko fjernet  Reduserer sannsynlighet  Reduserer alvorlighetsgrad  Reduserer konsekvens og sannsynlighet | Minimal  Betydelig (kan ikke slettes)  Ingen  Minimal  Mulig  Betydelig | Ja  Ja  Ja  Ja  Vurderes  Nei |

**4. Ledelsens validering av personvernkonsekvensvurderingen (DPIA)**

|  |  |  |
| --- | --- | --- |
| **Moment** | **Navn og dato** | **Kommentarer** |
| Tiltak godkjent av: |  |  |
| Restrisiko godkjent av: |  | *Dersom restrisiko med høy risikograd blir godkjent, ta kontakt med Datatilsynet før oppstart for forhåndsdrøfting, jf. art. 36 nr. 1.* |
| Personvernombudsbistand gitt: |  | *Personvernombudet skal gi råd om regelverksoverholdelse, steg 6-tiltak og om hvorvidt behandlingsaktiviteter kan settes i gang, jf. art. 35 nr. 2 og art. 39 nr. 1 bokstav c.* |
| Sammendrag av personvernombudets råd: | | |
| Personvernombudets råd er akseptert eller overprøvd av: |  | *Hvis overprøvd, må du forklare bakgrunnen for dette* |
| Kommentarer: | | |
| De registrertes synspunkter er innhentet og gjennomgått av: |  | *Hvis din avgjørelse avviker fra de registrertes synspunkter, bør du forklare bakgrunnen for at du velger å sette i gang/fortsette behandlingen* |
| Kommentarer: | | |
| Denne personvernkonsekvensvurderingen vil følges opp av: |  | *Personvernombudet bør også følge opp personvernkonsekvensvurderingen løpende, jf. art. 39 nr. 1 bokstav c.* |