Hvem er ansvarlig for personopplysninger i blokkjeder?

Identifisering av behandlingsansvarlig under GDPR i desentraliserte distribuerte databaser

Kandidatnummer: 37

Antall ord: 14 999

JUS399 Masteroppgave
Det juridiske fakultet

UNIVERSITETET I BERGEN

10. Desember 2019

The blockchain is part of the history of the Internet. It is at the same level as the WWW in terms of importance, and arguably might give us back the Internet, in the way it was supposed to be: more decentralized, more open, more secure, more private, more equitable, and more accessible.

- William Mougayar

Innholdsfortegnelse

Innholdsfortegnelse **2**
1 Innledning **4**
1.1 Tema og problemstilling 4
1.2 Rettskilder og metodiske utfordringer 6
1.3 Avgrensninger 8
1.4 Fremstillingen videre 9
2 General Data Protection Regulation **10**
2.1 Geografisk virkeområde 10
2.2 Saklig virkeområde 10
2.3 Sentrale aktører 11
3 Teknologien **14**
3.1 Innledning 14
3.2 P2P-nettverk 14
3.3 Den digitale hovedboken 16
3.4 Hash funksjoner 17
3.5 Asymmetrisk kryptering 18
3.5.1 Den offentlige nøkkelen representerer brukernavnet i nettverket 18
3.5.2 Den digitale signaturen beviser eierforhold 19
3.5.3 Lommebok 20
3.6 Blokkens struktur 20
3.7 Konsensusprotokoll 22
3.8 Smart kontrakt 23
4 Personopplysninger på blokkjeden **25**
4.1 Innledende om GDPRs saklige virkeområde 25
4.2 Behandles det personopplysninger på blokkjeden? 26
4.2.1 Innledning 26
4.2.2 Vilkåret "identifiserbar" opplysning 26
4.2.3 Identifiserer en offentlig nøkkel den registrerte? 29
4.2.4 Identifiserer transaksjonsdataen den registrerte? 30
5 Identifisering av behandlingsansvarlig **32**
5.1 Innledning 32
5.2 Vilkårene for identifisering av behandlingsansvarlig 33

5.2.1 Hvem kan være behandlingsansvarlig på blokkjeden? 33
5.2.2 Hvem bestemmer formålet med behandlingen og hvilke midler som skal benyttes? 33
5.2.3 Foreligger det felles behandlingsansvar? 36
6 Aktørenes ansvarsrolle på blokkjeden 39
6.1 Innledende om analysens utgangspunkt 39
6.2 Identifisering av ansvarsroller 39
6.2.1 Rollen til grunnleggeren og programvareutviklere 39
6.2.2 Rollen til brukerne av blokkjeden 41
6.2.3 Rollen til noder 46
6.2.4 Rollen til gruvearbeidere 47
6.2.5 Rollen til tilbydere av veksling- og oppbevaringstjenester 48
6.3 Problematikk knyttet til avtaleforhold mellom aktørene 49
6.3.1 Felles behandlingsansvar 49
6.3.2 Forholdet mellom behandlingsansvarlig og databehandler 51
7 Konklusjon og avsluttende betraktninger 53
Litteraturliste 55
7.1 Lover og forskrifter 55
7.2 EUs sekundærlovgivning 55
7.3 Rettspraksis fra EU-domstolen 55
7.4 Veiledere og uttalelser 56
7.5 Juridisk litteratur 57
7.5.1 Bøker 57
7.5.2 Artikler 57
7.5.3 Oppslagsverk 58
7.6 Veiledere, studier og rapporter 58
7.7 Øvrige kilder 59
7.7.1 Bøker 59
7.7.2 Nettsider 59
Lister over figurer 61

1 Innledning

1.1 Tema og problemstilling

I dagens moderne samfunn kontrolleres eierforhold i sentraliserte databaser[1]. Oversikt over eierforhold til eiendom og kjøretøy fremgår av henholdsvis tinglysningsregistrert og motorvognregisteret, mens banker holder oversikt over balansen til kontoeiere i sine databaser. Sentraliserte tredjeparter kontrollerer dermed «sannheten» om eierforhold. Blokkjeder kan imidlertid forstyrre og endre tankegangen om at «sannheten» må kontrolleres av sentraliserte mellommenn.[2]

Med blokkjeder menes desentraliserte distribuerte databaser hvor mellommannen er erstattet av et globalt nettverk av frivillige aktører som oppdaterer databasen i henhold til blokkjedens regler. Blokkjeder har potensiale til å erstatte mange av de sentraliserte databasene vi kjenner til i dag. Omlegging fra sentraliserte til desentraliserte distribuerte databaser kan sørge for økt effektivitet, transparens og lavere kostnader knyttet til endring av eierforhold.

Det er imidlertid uklarheter knyttet til hvorvidt opplysningene som behandles i blokkjeder er *personopplysninger*[3] og hvem som eventuelt er ansvarlig for disse. Ansvar for behandling av personopplysninger reguleres av General Data Protection Regulation[4] (heretter «GDPR», «personvernforordningen» eller «forordningen») som trådte i kraft for EU-landene 25. mai 2018[5] og i Norge 20. juli 2018 ved inkorporasjon gjennom EØS-avtalen.[6] GDPR opphevet personverndirektivet 1995[7] (heretter «personverndirektivet»). Temaet for denne avhandlingen er forholdet mellom ansvar for personopplysninger under GDPR og blokkjeder.

Bakgrunnen for ny personvernlovgivning i EU var den økte innsamlingen og utvekslingen av personopplysninger som er en konsekvens av den raske teknologiske utviklingen de siste 25 årene. Endringene skaper nye utfordringer med hensyn til vern av personopplysninger.[8] Formålet med forordningen er å bidra til harmonisering av personvernlovgivningen innenfor

[1] En database defineres i denne avhandlingen som «en samling data lagret på et elektronisk medium». Se Bratbergsengen (2019).
[2] Rode (2017).
[3] Definisjonen av personopplysninger presenteres i punkt 2.2 og mer inngående i punkt 4.2.
[4] EUROPAPARLAMENTETS- OG RÅDSFORORDNING (EU) 2016/579 av 27. April 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger samt om oppheving av direktiv 95/46/EF [GDPR].
[5] Jf. GDPR artikkel 99 nr. 2.
[6] Lov om behandling av personopplysninger 15. Juni 2018 nr. 31 (personopplysningsloven) § 1.
[7] EUROPAPARLAMENTETS- OG RÅDSDIREKTIV 95/46/EF av 24. Oktober 1995 om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger [Personverndirektivet].
[8] Jf. GDPR fortalepunkt 6.

EU.[9] Personvernlovgivningen ble dermed inntatt som forordning[10] ettersom det forelå forskjell i beskyttelsesnivå grunnet forskjellig gjennomføring og anvendelse av personverndirektivet.[11] Forordningen skal sikre balansen mellom et sikkert og ensartet personvern for borgere og fri flyt av personopplysninger i EU.[12]

GDPR ble utformet som et teknologisk nøytralt rammeverk som skulle være fleksibelt nok til å kunne tilpasse seg nyskapende teknologi. Forordningen bygger på grunnleggende personvernprinsipper som gir det fundamentale rammeverket for behandling av personopplysninger.[13] I henhold til ansvarsprinsippet i artikkel 5 nr. 2 er *behandlingsansvarlig*[14] overordnet ansvarlig for å overholde prinsippene og reglene i GDPR. Forordningen er dermed utformet med antagelse om at personopplysninger behandles i sentraliserte databaser med identifiserbare aktører.[15]

I blokkjeder er imidlertid den identifiserbare mellommannen erstattet av et globalt nettverk av frivillige ukjente aktører. Identifisering og fordeling av ansvar er allerede problematisk i sentraliserte databaser hvor flere aktører er involvert i behandlingen av personopplysningene. Problematikken forsterkes i blokkjeder ettersom behandlingen også desentraliseres. Problemstillingen i denne avhandlingen er hvorvidt en eller flere av aktørene involvert i behandlingen av personopplysninger på blokkjeder er behandlingsansvarlig. I lys av problemstillingen må det først avklares hvilke opplysninger på blokkjeder som omfattes av GDPR.

Uklarheten knyttet til ansvar for personopplysninger i en blokkjede gjør det utfordrende for tilsynsmyndighetene[16] å pålegge ansvar og for enkeltindivider å håndheve sine rettigheter.[17] Eksempelvis vil enkeltindividers rett til innsyn etter GDPR artikkel 15 være uten selvstendig betydning ettersom de ikke får tildelt en kontaktperson i henhold til informasjonsplikten i GDPR artikkel 13 og 14 som de kan håndheve sine rettigheter overfor.

[9] Skullerud mfl. (2018), s.35.
[10] En forordning gjelder som lov og kommer «direkte til anvendelse i alle medlemsstatenes interne rettsordener», i motsetning til et direktiv som kun gir et «pålegg til medlemsstatene om å vedta nasjonale regler med et visst innhold innen en angitt tidsfrist», se Fredriksen & Mathisen (2014) s. 22-23.
[11] Jf. fortalepunkt 9.
[12] Jf. fortalepunkt 10.
[13] Jf. artikkel 5.
[14] Definisjonen av behandlingsansvarlig presenteres i punkt 2.3 og mer inngående i punkt 5.2.
[15] Se også fortalepunkt 79.
[16] Jf. artikkel 51.
[17] Se GDPR kapittel 3.

Et usikkert regulatorisk landskap for blokkjedeteknologi kombinert med høye satser for overtredelsesgebyr[18] kan i tillegg påvirke innovasjon og masseadopsjon av blokkjedeteknologi. En avklaring av hvilke opplysninger i blokkjeden som omfattes av GDPR og den juridiske statusen til aktørene i blokkjeder vil gi forutsigbare regulatoriske rammer som vil ha betydning for økt innovasjon av blokkjeder.

Europakommisjonen har planer om å investere 300 millioner euro i blokkjede-prosjekter frem mot 2020 og satser dermed tungt for å bli en ledende aktør innen feltet.[19]. I april 2018 ble European Blockchain Partnership opprettet og består av 27 medlemsland i EU, samt Norge og Liechtenstein, som skal jobbe sammen for å utvikle infrastruktur som for å levere tjenester innenfor EU ved bruk av blokkjedeteknologi.[20]

1.2 Rettskilder og metodiske utfordringer

Hovedutfordringen med oppgaven er mangelen på autoritative rettskilder som kan bidra til å avklare forholdet mellom jussen og teknologien. Det vil i det følgende redegjøres for rettskildene som er relevante for å analysere avhandlingens juridiske problemstilling.

Oppgavens primære rettskilde er GDPR. Forordningen «gjelder som lov», jf. personopplysningsloven § 1. Den norske oversettelsen av GDPR vil være den primære rettskilden og alminnelig juridisk metode benyttes i analysen. Bestemmelsene i GDPR tolkes i lys av forordningens overordnede formål inntatt i GDPR artikkel 1.[21]

Forordningens *fortale* begrunner både forordningens individuelle bestemmelser og selve rettsaktens formål.[22] Fortalen er ikke juridisk bindende[23], men gir uttrykk for formålet bak forordningens bestemmelser og fungerer derfor som viktig tolkningshjelp ved mangel på andre klare rettskilder.

Det er ingen avgjørelser avsagt i *Den europeiske unions domstol* (heretter «EU-domstolen») som vurderer forholdet mellom GDPR og blokkjeder. Imidlertid vil enkelte avgjørelser fra EU-

[18] Etter GDPR artikkel 83 nr.5 kan tilsynsmyndighetene ilegge overtredelsesgebyr på opptil 20 millioner euro eller, dersom det dreier seg om et foretak, på opptil 4 % av den samlede global omsetningen..
[19] Europakommisjonen (2018).
[20] Europakommisjonen (2019).
[21] Skullerud mfl. (2018) s.41.
[22] Fredriksen & Mathisen (2014) s.228.
[23] Jf. C-345/13, avsnitt 31: « […] it should be borne in mind that the preamble to a Community act has no binding legal force and cannot be relied on either as a ground for derogating from the actual provisions of the act in question or for interpreting those provisions in a manner clearly contrary to their wording".

domstolen benyttes ved tolkning av definisjonene i GDPR ettersom bestemmelsene som analyseres i oppgaven viderefører i stor grad definisjonene i personverndirektivet. Dette medfører at EU-domstolens avgjørelser knyttet til personverndirektivet er relevante for tolkning av de sammenfallende definisjonene i GDPR. Hvilke bestemmelser som er sammenfallende med personverndirektivet påpekes underveis i oppgaven.

Article 29 Working Party (heretter «Artikkel 29-gruppen») var EUs rådgivende organ i personvernspørsmål frem til implementering av GDPR i medlemsstatene.[24] Uttalelsene til Artikkel 29-gruppen er ikke juridisk bindende, men fungerer som et viktig hjelpemiddel for å forstå innholdet i og sammenhengen mellom artiklene.[25]

Artikkel 29-gruppens arbeid ble den 25. mai 2018 videreført i *European Data Protection Board* (heretter «Personvernrådet») som skal sikre ensartet anvendelse av forordningen, jf. artikkel 70 nr. 1. Personvernrådet, i likhet med Artikkel-29 gruppen, består av en representant fra de nasjonale datastilsynsmyndighetene, jf. artikkel 68 nr. 3. Personvernrådet har gitt ut begrenset med eget materiale, men har gitt sin tilslutning til flere av Artikkel-29 gruppen sine veiledere.[26] Veilederne som benyttes i avhandlingen er ikke videreført av EDPB, men ettersom definisjonene videreført i GDPR er sammenfallende med definisjonene i personverndirektivet ansees de fremdeles relevante for analysen.

Retningslinjer fra tilsynsmyndigheter vil anvendes som en supplerende informasjonskilde i avhandlingen, særlig fra det franske datatilsynet Commision Nationale de l'Informatique et des Libertés[27] (CNIL). CNIL ble 6 november 2018 den første tilsynsmyndigheten i Europa til å utgi en veiledning om forholdet mellom blokkjeder og GDPR.[28]

Flere EU-institusjoner har utgitt en rekke rapporter og studier om forholdet mellom GDPR og blokkjeder. I februar 2018 opprettet Europakommisjonen, i samarbeid med Europaparlamentet, *the European Blockchain and Observatory Forum* (heretter «EBOF»), som har samlet ledende eksperter på området og utgitt en rekke rapporter om forholdet mellom GDPR og blokkjeder. I juli 2019 ga Europaparlamentet ut en studie om GDPR kan anvendes på blokkjeder (heretter «Europaparlamentets studie fra 2019») skrevet av *the Panel for the Future of Science and*

[24] Wessel-Aas & Ødegaard (2018) s.94.
[25] Ibid.
[26] Oversikt over veiledere EDPB har gitt tilslutning til er tilgjengelig på: https://edpb.europa.eu/news/news/2018/endorsment-gdpr- wp29-guidelines-edpb_en.
[27] https://www.cnil.fr/.
[28] CNILs veileder om blokkjeder (2018).

Technology (STOA)[29]. Selv om retningslinjene har lite rettskildemessig vekt, vil de trekkes frem og supplere argumentasjonen.

Enkelte uttalelser og synspunkter i *juridisk litteratur* vil benyttes hvor disse har argumentasjonsverdi. Flere *internasjonale juridiske artikler* behandler spørsmålet om forholdet mellom GDPR og blokkjeder, og disse synspunktene og uttalelsene vil trekkes frem i mangel på andre autoritative rettskilder.

Grunnet avhandlingens tema vil *ikke-juridiske kilder* anvendes for å forklare teknologien. Slike kilder anses som nødvendig for å kunne gi en grunnleggende forklaring av teknologien som er nødvendig for å kunne analysere definisjoner i forordningen.

1.3 Avgrensninger

Hovedformålet med oppgaven er vurdere hvorvidt det er mulig å identifisere hvilke aktører på blokkjeden som innehar rollen som behandlingsansvarlig, og eventuelt databehandler, i henhold til GDPR. Forpliktelsene til behandlingsansvarlig fremgår av forordningens enkelte bestemmelser, og noen kan være vanskelig, om ikke umulig, å overholde i lys av blokkjedens fundamentale egenskaper. Imidlertid skal oppgaven *kun* avklare ansvarsrollene til aktørene på blokkjeden, og ikke hvordan og hvorvidt aktørene har mulighet til å overholde prinsippene og forpliktelsene i GDPR.

Blokkjeder kan hovedsakelig deles inn to ulike kategorier; åpne offentlige blokkjeder og private lukkede blokkjeder. Den grunnleggende teknologien er lik i begge tilfellene, men det er forskjeller i tilgangsrettigheter og hvilke aktører som kan validere transaksjoner på blokkjeden. Formålet med åpne offentlige blokkjeder er å desentralisere databasen. Databasen er dermed offentlig tilgjengelig og det finnes ingen sentralisert aktør med utøvende makt. I en privat lukket blokkjede er tilgangen og valideringen av transaksjoner begrenset av visse aktører i nettverket.

Ettersom det er enklere å fordele ansvar og etablere avtaleforhold mellom aktørene i en privat lukket blokkjede, er det de åpne offentlige blokkjeder som representerer de største utfordringene ved overholdelse av GDPR.[30] Avhandlingen vil *kun* fokusere på forholdet

[29] STOA (2019).
[30] Ibid. s.1.

mellom GDPR og åpne offentlige blokkjeder, og det avgrenses følgelig mot lukkede private blokkjeder.

Oppgaven vil redegjøre for de tekniske egenskapene til blokkjeder i den grad det er nødvendig for å forstå problematikken og spenningene mellom teknologien og GDPR. Avhandlingen er en juridisk analyse, og ikke ment å analysere teknologiske aspekter i særlig detalj.

Teknologien i blokkjeder ble introdusert i 2008 og det har i etterkant blitt opprettet mange nye blokkjeder med ulike funksjoner og egenskaper på grunnlag av den opprinnelige kildekoden. Bitcoin- og Ethereum er de mest kjent blokkjedene og det vil dermed vil fokuseres på de teknologiske elementene som finnes i dem. Følgelig avgrenses det mot nye teknologier under utvikling og teknologier på andre blokkjeder.

Det vil hovedsakelig brukes eksempler tilknyttet overføring av eierskap og finansielle instrumenter i avhandlingen. Selv om blokkjeder ansees å få stor innflytelse innenfor mange sektorer, har de fått størst fotfeste innenfor finansbransjen.

Oppgaven baserer seg på rettskildebildet slik det var 2. desember 2019.

1.4 Fremstillingen videre

Før avhandlingen redegjør for selve teknologien, vil det i *kapittel to* gis en kort redegjørelse for sentrale begrep og aktører i GDPR som er relevante i vurderingen om hvilke opplysninger på blokkjeden som omfattes av GDPR og identifisering av aktørenes ansvarsroller på blokkjeden.

I *kapittel tre* vil teknologien og reglene som sikrer dataens integritet i et desentralisert og distribuert nettverk forklares. Ettersom avhandlingens problemstilling knytter seg til en ny og relativt ukjent teknologi er det hensiktsmessig å redegjøre for teknologien i den grad det er nødvendig for å forstå problemstillingene teknologien reiser i forhold til GDPR.

I *kapittel fire* vil det først redegjøres for i hvilken grad opplysninger som behandles i blokkjeder er personopplysninger. Denne vurderingen er nødvendig for å kunne angi hvorvidt GDPR i det hele tatt kommer til anvendelse. Deretter vil det i *kapittel fem* gjøres rede for vilkårene for å identifisere behandlingsansvarlig på blokkjeden, før det i *kapittel seks* vurderes om aktørene involvert i behandling av opplysninger på blokkjeden er behandlingsansvarlige. Avslutningsvis i *kapittel syv* oppsummeres funnene i oppgaven.

2 General Data Protection Regulation

2.1 Geografisk virkeområde

Personvernforordningens geografiske virkeområde ble utvidet med GDPR artikkel 3 og får virkning for virksomheter lokalisert innenfor EU, men også for virksomheter utenfor EU som tilbyr varer og tjenester til borgere i EU. GDPRs geografiske virkeområde er dermed svært omfattende og er «i praksis globale regler for aktører som retter sin virksomhet mot EU og/eller EØS-området».[31] Formålet med utvidelsen er å gi et omfattende personvern for EU borgere.

Et blokkjede-nettverk er på lik måte som internett satt sammen av et globalt nettverk av aktører spredt på tvers av landegrenser. GDPRs vide geografiske virkeområde gjør dermed problematikken vedrørende identifisering av ansvar for personopplysninger i blokkjeder enda mer aktuell.

2.2 Saklig virkeområde

Personvernforordningens saklige virkeområde fremgår av GDPR artikkel 2 nr. 1. Etter bestemmelsen kommer GDPR til anvendelse på «helt eller delvis automatisert behandling av personopplysninger […] som inngår eller skal inngå i et register». Virkeområdet til forordningen er svært vid og det må avklares om anvendelse av blokkjeder omfattes av GDPR.

I det følgende vil det redegjøres for de mest sentrale begrepene knyttet til vurderingen om anvendelse av blokkjeder omfattes av GDPR. Begrepet *personopplysning* vil drøftes mer inngående i punkt 4.2.

En **personopplysning** defineres i GDPR artikkel 4 nr. 1 som «enhver opplysning om en identifisert eller identifiserbar fysisk person». Med den «registrerte» siktes det til den fysiske personen som identifiseres av opplysningene. Ordlyden «enhver opplysning» tilsier at definisjonen omfavner vidt. I Peter Nowak-dommen[32] støttet EU-domstolen seg til en slik forståelse i lys av «it reflects the aim of the EU legislature to assign a wide scope to that concept». Uttalelsen innebærer at definisjonen skal forstås vidt for å omfatte alle former for

[31] Wessel-Aas & Ødegaard (2018) s.25.
[32] Sak C-434/16, avsnitt 34.

opplysninger som kan identifisere en fysisk person. En slik forståelse gir et omfattende vern for den registrerte i tråd med forordningens formål om å gi borgere effektivt og sikkert personvern.

Begrepet **behandling** defineres i GDPR artikkel 4 nr. 2 som «enhver operasjon eller rekke av operasjoner som gjøres med personopplysninger, enten automatisert eller ikke […]». Bestemmelsen viser til eksempler på hva som kan være behandling, som blant annet innsamling, registrering, organisering, strukturering, lagring og utlevering. Opplistingen av eksempler er ikke uttømmende. Ordlyden omfavner vidt og tilsier at enhver befatning med personopplysninger er omfattet. Fortalepunkt 15 presiserer at «[f]or å unngå at det oppstår en alvorlig risiko for at bestemmelsene omgås bør vernet av fysiske personer være teknologinøytralt og ikke avhenge av teknikkene som benyttes». Definisjonen skal dermed tolkes vidt for å gi «fleksibilitet til å møte nye behandlingsmåter som følge av den teknologiske utviklingen».[33]

GDPR artikkel 4 nr. 5 definerer **pseudonymisering** som «behandling av personopplysninger på en slik måte at personopplysningene ikke lenger kan knyttes til en bestemt registrert uten bruk av tilleggsopplysninger, forutsatt at disse tilleggsopplysningene lagres atskilt og omfattes av tekniske og organisatoriske tiltak som sikrer at personopplysningene ikke kan knyttes til en identifisert eller identifiserbar fysisk person». Det fremgår av fortalepunkt 26 at pseudonymiserte personopplysninger ansees som «personopplysninger» i henhold til GDPR artikkel 4 nr. 1. Pseudonymisering er følgelig en måte å behandle personopplysninger på, og ikke en egen kategori med personopplysninger.

2.3 Sentrale aktører

Effektiv identifikasjon og tydelig fordeling av ansvar hos aktører som behandler personopplysninger står sentralt, både for at den registrerte skal kunne utøve sine rettigheter overfor aktørene, samt at tilsynsmyndighetene kan pålegge ansvar hos virksomheter som ikke etterfølger forpliktelsene i forordningen, jf. fortalepunkt 79.

GDPR skiller hovedsakelig mellom to aktører som behandler personopplysninger; behandlingsansvarlig og databehandler. Definisjonene er sentrale i den videre analysen om den

[33] Skullerud mfl. (2018) s.44.

juridiske statusen til aktørene på blokkjeden. Begrepet *behandlingsansvarlig* vil drøftes mer inngående i punkt 5.2.2.

En **behandlingsansvarlig** defineres i artikkel 4 nr. 7 som en «fysisk eller juridisk person, en offentlig myndighet, en institusjon eller ethvert organ» som «alene eller sammen med andre» «bestemmer formålet med behandlingen av personopplysninger og hvilke midler som skal benyttes». Behandlingsansvar kan oppstå som følge av rettslig kompetanse, faktiske beslutninger eller som følge av lov.[34]

EU-domstolen uttalte i Google Spain-dommen[35] at definisjonen skal tolkes vidt for å sikre en «effective and complete protection of data subjects». Denne forståelsen har EU-domstolen gjentatt i etterkant av Google Spain-dommen, senest i den nylig avsagte Fashion ID-dommen[36] hvor det ble uttalt at definisjonen skal forstås vidt for å sikre «a high level of protection of the fundamental rights and freedoms of natural persons». Uttalelsene tilsier en vid forståelse av vilkårene i artikkel 4 nr. 7 for å hindre omgåelse av personvernlovgivningen og sikre en effektiv beskyttelse for de registrerte.

En aktør som identifiseres som behandlingsansvarlig må i henhold til prinsippet om lovlighet i artikkel 5 nr. 1 sørge for at det foreligger et rettslig grunnlag for å kunne behandle personopplysninger i tråd med forordningen. GDPR artikkel 6 angir seks alternative grunnlag for behandlingen som for eksempel den registrertes samtykke[37], når behandling er nødvendig for å oppfylle en kontrakt med den registrerte[38] eller nødvendig for å ivareta den berettigede interessen til behandlingsansvarlig når den ikke overstiger personverninteressen til den registrerte.[39]

Ordlyden «alene eller sammen med andre» i artikkel 4 nr. 7 indikerer at flere kan være behandlingsansvarlige sammen. En slik ordning er definert i GDPR som ***felles behandlingsansvar*** og er nedfelt i artikkel 26 nr. 1. Det fremgår av bestemmelsen at felles behandlingsansvar foreligger «dersom to eller flere behandlingsansvarlige i fellesskap fastsetter formålene med og midlene for behandlingen». Formålet bak GDPRs definering av felles

[34] A29 WP Opinion 1/2010, s. 10-11 og Skullerud mfl. (2018) s.60.
[35] Sak C-131/12, avsnitt 34.
[36] Sak C-40/17, avsnitt 65.
[37] Jf. artikkel 6 nr. 1 bokstav a.
[38] Jf. artikkel 6 nr. 1 bokstav b.
[39] Jf. artikkel 6 nr. 1 bokstav f.

behandlingsansvar må sees i lys av stadig mer teknologisk komplekse nettverk hvor personopplysninger behandles av flere behandlingsansvarlige.

En behandlingsansvarlig kan velge å sette ut hele eller deler av behandlingen til en annen aktør.[40] Aktøren defineres som en ***databehandler*** i GDPR artikkel 4 nr. 8 og behandler personopplysninger «på vegne» av den behandlingsansvarlige. Ordlyden «på vegne» i artikkel 28 nr. 1 indikerer at databehandleren behandler personopplysninger for en annen aktør. Bestemmelsen må sees i lys av at databehandler skal bare behandle personopplysninger «etter instruks fra den behandlingsansvarlige», jf. artikkel 29.

Konsekvensene av at databehandler ikke lenger behandler personopplysninger «på vegne» av behandlingsansvarlig, men fastsetter formålene med og midlene for behandlingen selv, er at databehandler anses som behandlingsansvarlig for den konkrete behandlingen, jf. artikkel 28 nr. 10.

Forholdet mellom behandlingsansvarlig og databehandler skal være «underlagt en avtale eller annet rettslig dokument» i henhold til artikkel 28 nr. 3. Dette omtales som en databehandleravtale.

[40] Olsen (2018).

3 Teknologien

3.1 Innledning

I oktober 2008 publiserte pseudonymet Satoshi Nakamoto artikkelen «Bitcoin: A Peer-to-Peer Electronic Cash System» som introduserte en ny teknologi – blokkjeden- som tillot digitale verdier å bli sendt direkte mellom to parter uten å måtte valideres av en mellommann.[41] Blokkjedens digitale verdi ble kalt Bitcoin. De underliggende teknologiene til Bitcoin-blokkjeden eksisterte allerede, men sammensetningen var revolusjonerende.

Teknologien har utviklet seg fra å være en plattform for overføring og registrering av transaksjoner, til å også tjene som infrastruktur for desentraliserte applikasjoner som fasiliterer overføringen av dokumenter, eiendom og andre verdier.[42] Ethereum blokkjeden, med den tilhørende digitale verdien Ether, er et eksempel på utviklingen fra Bitcoin-blokkjeden.[43]

Det finnes ikke en formell definisjon av *blokkjeder* i EU- og EØS retten og det vises dermed til en mer formell definisjon fra Europaparlamentet. I Europaparlamentets studie fra 2019 defineres blokkjeden som en "[…] delt og synkronisert digital database som er vedlikeholdt av en konsensusalgortime og lagret på et flertall av noder (datamaskiner som lagrer en lokal versjon av databasen)».[44]

I dette kapittelet forklares de underliggende teknologiene i blokkjedene som grunnlag for de rettslige drøftelsene.

3.2 P2P-nettverk

Alle nettverk trenger et programvaresystem for å kunne kommunisere med hverandre over internett. Et nettverk er satt sammen av *noder* som er individuelle datamaskiner på samme nettverk som kjører en spesifikk programvare. Arkitekturen til programvaresystemet kan

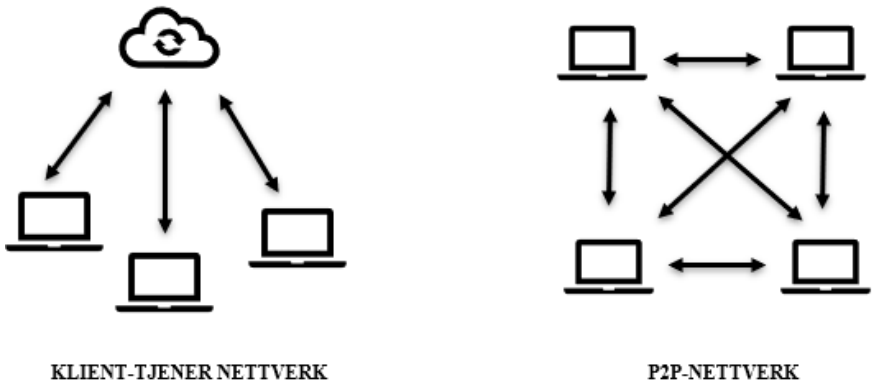
[41] Nakamoto (2008) s.1.
[42] STOA (2019) s.4.
[43] Se punkt 3.9 om egenskapen til Ethereum-blokkjeden.
[44] STOA (2019) s.3. Sitat oversatt fra engelsk: «In essence, a blockchain is a shared and synchronised digital database that is maintained by a consensus algorithm and stored on multiple nodes (computers that store a local version of the database).

designes sentralisert eller distribuert.[45] Dersom en enkeltstående svikt i systemet medfører stopp i driften av nettverket, er ikke systemet distribuert.[46]

Den tradisjonelle databasen i dag er sentralisert og kalles for et klient-tjener-nettverk. Nodene (klienten) er koblet over et nettverk til en sentral server som behandler nodenes data. Nodene er avhengig av serveren for få tilgangsrettigheter til informasjonen lagret på serveren.

Motsetningsvis er distribuert database teknologi en database som er spredt over flere noder i et stort nettverk, men administreres som ett system.[47] Blokkjeder er den mest kjente distribuerte database teknologien. En distribuert database trenger et *fildelingsnettverk*, samt en *konsensusalgortime*[48] for å sikre at nodene er enige om innholdet i databasen.[49] Blokkjeder bruker et fildelingsnettverk kalt *peer-to-peer-nettverk* (heretter «P2P-nettverk»). Begrepet «peer-to-peer» innebærer at nodene som deltar i nettverket er likestilte, med tilsvarende rettigheter og roller.[50] Alle nodene er både leverandører og brukere av dataressurser.[51]

Alle har mulighet til å delta i blokkjedens P2P-nettverk. Dette gjøres ved å laste ned en programvare som kobler datamaskinen til blokkjeden og datamaskinen blir en node i blokkjede-nettverket. Det finnes ingen nettverkseier, ingen registreringsprosedyrer, ingen registrering og ingen begrensninger for hvem som kan delta i blokkjeden.[52]



Figur 1 sammenligner et P2P-nettverk med et sentralisert nettverk hvor alle enhetene er tilkoblet en sentralisert server[53]

[45] Drescher (2017) s.15.
[46] Ibid. s.16.
[47] Skramstad (2015).
[48] Se punkt 3.7.
[49] Ray (2018).
[50] Drescher (2017) s.15.
[51] Ibid.
[52] EBOF (2018) s.14.
[53] Inspirasjon for figuren er hentet fra Lastovetska (2019).

3.3 Den digitale hovedboken

Den digitale *hovedboken* er en database som holder en tidsstemplet oversikt over transaksjoner fra tidspunktet blokkjeden opprettes. Hver node i nettverket har en oppdatert kopi av hovedboken. Nodene kan velge å delta i nettverket på ulike måter – som *fullverdig node* eller *deltakernode.*[54]

Fullverdige noder laster ned hele hovedboken og validerer transaksjoner. En fullverdig node kan også velge å kjøre en spesiell form for fullverdig node kalt en *gruvearbeider.*[55] Deltakernoden laster ikke ned hele blokkjeden, men kun delen som er relevant for å godta de fullverdige nodenes validering av transaksjoner.[56] I tillegg kan nettklienter –som ikke har lastet ned programvaren – få tilgang til hovedboken gjennom en tredjepartstjenestes nettleser.[57]

Fordelen av oppdaterte kopier av hovedboken distribuert over et nettverk, istedenfor kun *en* sentral hovedbok, er at det ikke finnes et enkeltpunkt for feiling. Dersom hovedboken hos en node blir forsøkt ødelagt, destruert eller forfalsket vil ikke dette være av betydning ettersom dokumentasjonen – «sannheten» - ligger tilgjengelig hos alle de andre nodene i nettverket.[58]

Hovedboken oppdateres av blokkjedens *protokoll* som angir reglene aktørene på blokkjeden må følge for å sikre eierhold i et distribuert P2P-nettverk. Dette er regler som angir blant annet hvordan brukere oppretter en transaksjon, hvordan transaksjoner samles i blokker og hvordan fullverdige noder skal validere transaksjoner.[59] Protokollen sikrer at alle nodene i nettverket er enige om oppdateringer til hovedboken og oppdaterer sin lokale kopi av blokkjeden. Denne prosessen vil forklares nærmere i punkt 3.7.

Protokollen sikrer dermed blokkjedens integritet ved fravær av en mellommann som kan verifisere at transaksjonen er gyldig. Michele Finck (medlem av EBOF) presiserer at « […] blockchains do not make trust disappear; they simply replace trust in humans and institutions with trust in technology”.[60]

[54] Bacon mfl. (2018) s.19.
[55] Se punkt 3.7.
[56] Bacon mfl. (2018) s.19.
[57] Antonopoulos (2015) s 6.
[58] Drescher (2017) s.47.
[59] Buocz mfl. (2019) s.195.
[60] Finck (2019) s.13.

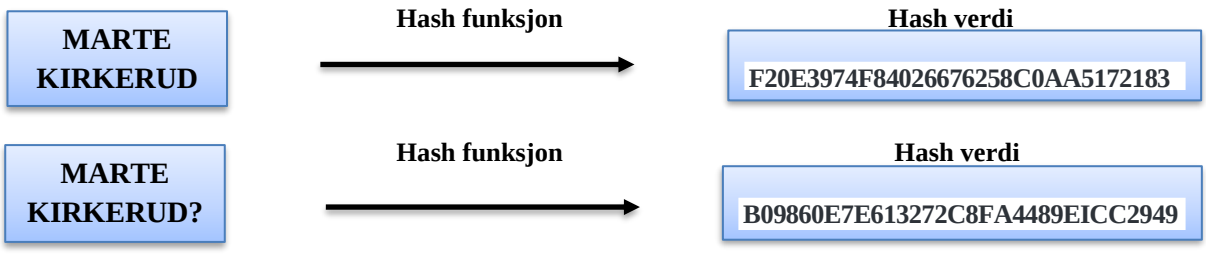
Den opprinnelige protokollen til blokkjeden designes av *protokollutvikleren* – også kalt *grunnleggeren* av blokkjeden – som bestemmer hvilke regler protokollen skal angi for å oppfylle formålet med blokkjeden. Protokollen (programvaren) oppdateres og vedlikeholdes av *programvareutviklere*.[61] Insentivet for å bidra som en programvareutvikler er å vedlikeholde eller utvikle plattformen, og dermed øke muligheten for at den digitale verdien tilhørende blokkjeden øker i verdi.[62]

Nodene kan velge å avslå programvareoppdateringene som fører til en *hard fork*, det vil si en konkurrende blokkjede bygget på samme åpne kildekode.[63] En nærmere forklaring av egenskapen er ikke relevant, men det er viktig å forstå at noder kan velge å avslå programvareoppdateringer.

3.4 Hash funksjoner

Hash funksjoner – også kalt *hashing* – er en teknologi (matematisk program) som sikrer dataens integritet på blokkjeden. Data som hashes kommer ut som et unikt fingeravtrykk bestående av en rekke bokstaver og tall. Dette fingeravtrykket kalles en *hash verdi*.[64] Hashet data viser alltid tilsvarende hash verdi. Dette innebærer at hvis to eller flere hash verdier i hovedboken er identiske, så er dataen helt identisk.

Eksempelvis vil teksten «Marte» og «Marte» alltid gi denne samme hash verdien. Imidlertid vil hash verdien endres hvis noen endrer dataene. Endres teksten fra «Marte» til «Marte?» endres også hash verdien. Følgelig sikrer hash verdien dataens integritet på blokkjeden ved å avsløre hvorvidt dataen som er registrert har blitt endret.



Figur 2 illustrerer at data som kjøres gjennom en hash funksjon, endres til en rekke bokstaver og tall som kalles en hash verdi.

[61] EBOF (2019) s.16.
[62] Bacon mfl. (2018) s.34.
[63] Ibid.
[64] Finck (2019) s.7.

Hashing er en enveis-funksjon som innebærer at det ikke er mulig å gjenopprette de opprinnelige dataene, i motsetning til asymmetrisk kryptering som det skal redegjøres for i punkt 3.5.[65] Det finnes ulike type hash funksjoner som reduserer en hvilken som helst mengde data ned til en viss størrelse.[66] Hashing medfører at Marte Kirkerud kan overføre data til Peder Ås uten at informasjonen publiseres i den offentlige databasen, men kun referansen til informasjonen.

3.5 Asymmetrisk kryptering

Kryptering er den digitale ekvivalenten til å låse en dør med en nøkkel (beskytte data), mens dekryptering er den digitale ekvivalenten til å bruke en nøkkel til å åpne døren.[67] Blokkjeder bruker *asymmetrisk kryptering* for å bevise eierskap til eiendelen som skal overføres via blokkjede-plattformen uten å begrense blokkjedens offentlige distribuerte arkitektur.[68]

Asymmetrisk kryptering innebærer at to nøkler – en offentlig og en privat nøkkel - genereres samtidig ved hjelp av kryptografisk programvare.[69] Nøklene har et matematisk forhold som innebærer at tekst kryptert med den offentlige nøkkelen kan *kun* dekrypteres av den private nøkkelen, og motsatt.[70]

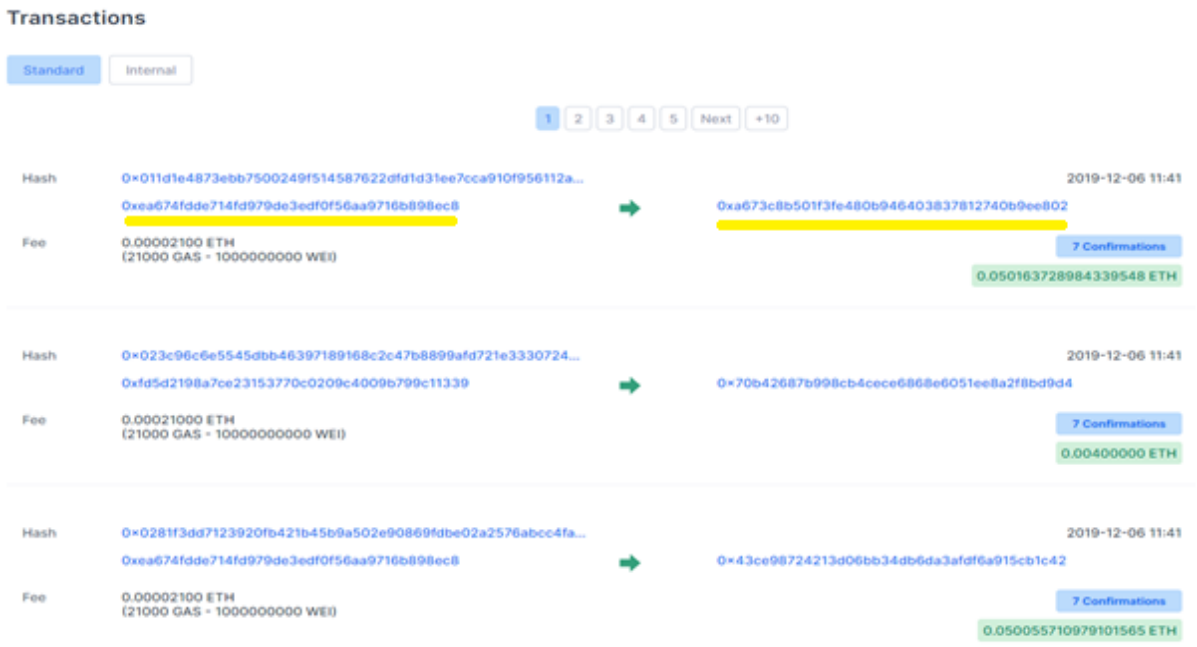
For å belyse forholdet mellom nøklene vises til det følgende eksempel: Marte ønsker å sende meldingen «Jeg forlater mannen min» til sin kjæreste Ole over en blokkjede. Istedenfor å sende beskjeden i vanlig tekst, krypterer Marte teksten med Ole sin offentlige nøkkel før den registreres på blokkjeden. Beskjeden kan kun dekrypteres med Oles private nøkkel. Martes ektemann Peder har mistanker om at hun er utro med Ole. Selv om Peder kjenner til Ole sin offentlige nøkkel, vil han kun klare å dekryptere teksten hvis han er i besittelse av Oles private nøkkel.

3.5.1 Den offentlige nøkkelen representerer brukernavnet i nettverket

Formålet med en offentlig nøkkel er i blokkjedesammenheng å representere den fysiske eller juridiske personen i nettverket med den korresponderende private nøkkelen.[71] Nodene som

[65] Ibid. s.91
[66] Ibid.
[67] Drescher (2017). s. 95.
[68] Ibid. s. 94.
[69] Ibid. s. 96.
[70] STOA (2019) s. 26.
[71] Bacon mfl. (2018) s. 14-15.

verifiserer transaksjoner må kunne identifisere brukerne på nettverket for å opprettholde kartleggingen mellom eier og eiendom. Brukere kan generere så mange offentlige nøkler som de selv ønsker, som korresponderer med den private nøkkelen.[72]



Figur 3 illustrerer de individuelle transaksjonene i en blokk og viser hvordan offentlige nøkler representerer brukerne på blokkjeden. Den offentlige nøkkelen til sender og mottaker er understreket i gult.[73]

Figur 3 illustrerer at aktørene i nettverket ikke representeres med egne navn, eksempelvis Marte Kirkerud eller martekirkerud@gmail.com, men av bokstavene og tallene i den offentlige nøkkelen. Det vil redegjøres for i punkt 4.2.3 hvorvidt offentlige nøkler er *personopplysninger* i henhold til GDPR artikkel 4 nr. 1.

3.5.2 Den digitale signaturen beviser eierforhold

Asymmetrisk kryptering brukes også for å signere en transaksjon med den private nøkkelen, og verifisere transaksjonen med den offentlige nøkkelen. Den private nøkkelen er dermed brukerens tilgang til blokkjeden.[74] Eksempelvis ønsker Marte å sende 500 Ether til Peder. Transaksjonen består av Martes beskjed «500 Ether til Peder» og Peder sin offentlige nøkkel. Marte krypterer disse opplysningene med hennes private nøkkel. Dette gir en digital signatur som verifiserer at transaksjonen kom fra Marte.

[72] Ibid. s.44.
[73] Figuren er et skjermutklipp fra Ethereum-blokkjeden tilgjengelig på: https://www.blockchain.com/explorer?view=eth_blocks
[74] Bacon mfl. (2018) s.44.

Etter at Marte signerer transaksjonen med sin digitale signatur kringkastes transaksjonen til nettverket og alle nodene får beskjed om at eiendelen skal skifte eier. Nodene sjekker hovedboken med alle registrerte transaksjoner og verifiserer at den som eier den offentlige nøkkelen greier å signere transaksjonen med sin korresponderende private nøkkel.[75]

3.5.3 Lommebok

Ønsker Marte å bruke blokkjeden for å overføre, motta eller lagre eiendeler må hun laste ned en programvare som oppbevarer hennes private nøkkel og alle offentlige nøkler. Denne programvaren kalles på blokkjeden for en *lommebok.*[76] En fullverdig node laster ned lommebok-programvaren når hele blokkjeden lastes ned og kan initiere transaksjoner direkte til nettverket.[77] En deltakernode laster ned lommebok-programvaren, men er avhengig av servere drevet av tredjeparter[78] for å få tilgang til transaksjonene på blokkjeden da den ikke laster ned hele blokkjeden, som nevnt i punkt 3.3.[79]

Alle blokkjeder har en digital verdi som defineres som *virtuell valuta,* jf. hvitvaskingsforskriften 2018[80] § 1-3. Etter bestemmelsen er virtuell valuta «et digitalt uttrykk for verdi, som ikke er utstedt av en sentralbank eller offentlig myndighet, som ikke nødvendigvis er knyttet til en offisiell valuta, og som ikke har rettslig status som valuta eller penger, men som aksepteres som betalingsmiddel, og som kan overføres, lagres eller handles elektronisk".

3.6 Blokkens struktur

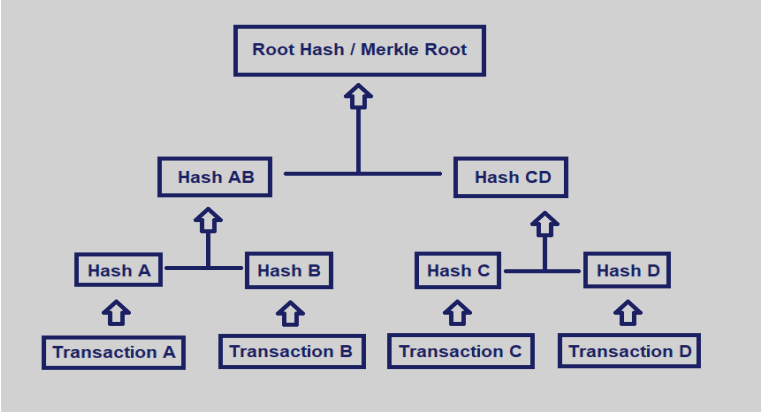
Transaksjoner i blokkjeden samles i en blokk. En blokk er en datastruktur som brukes for å holde på transaksjonene som kringkastes ut til nettverket av brukerne. Når en blokk legges til blokkjeden identifiseres den av sin hash verdi. Blokkens hash verdi består *av blokk-overskriften* og *blokk-kroppen* som har blitt påført en hash-funksjon.[81]

Blokk-kroppen består av transaksjonsdataen som er samlet i blokken. Det vil redegjøres for i punkt 4.2.4 om transaksjonsdata er *personopplysninger* i henhold til GDPR artikkel 4 nr. 1.

[75] Ibid. s. 15.
[76] Antonopoulos (2015) s. xxi.
[77] Ibid. s. 6.
[78] Se punkt 6.2.5 for definisjonen av tredjepartstjenester.
[79] Antonopoulos (2015) s. 6
[80] Forskrift om tiltak mot hvitvasking og terrorfinansiering (hvitvaskingsforskriften) 14. September 2018 nr. 1324.
[81] Bacon mfl. (2018) s. 12-13.

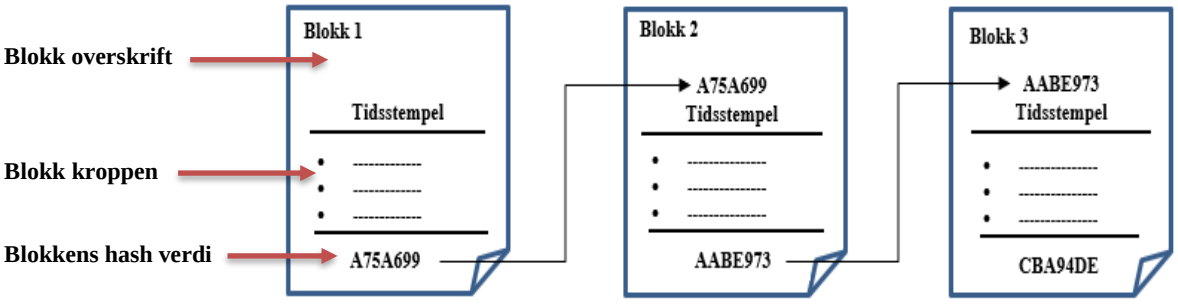
Blokkens hash verdi peker på roten til et Merkle-tree som er navnet på datastrukturen som brukes for å samle transaksjoner i en blokk.[82] Datastrukturen brukes for at nodene kan effektivt oppsummere hash verdien til store mengder individuelle transaksjoner.

Det er ikke relevant for oppgavens problemstilling å redegjøre for hvordan et Merkle-tree fungerer i praksis, men det er viktig å påpeke at hver blokk på en blokkjede ikke består av *en* transaksjon, men *flere* transaksjoner som sendes ut i nettverket av ulike brukere. Det vises likevel til figur 4 for å illustrere hvordan transaksjoner i blokkjeden samles i en blokk.



Figur 4 illustrer hvordan transaksjonene fra A, B, C og D er samlet i en datastruktur i blokken kalt et Merkle-tree.[83]

Blokk-overskriften består av en *hash referanse* og metadata som blant annet et tidsstempel.[84] Hash referansen er hash verdien til den tidligere blokken på blokkjeden og blokker er lenket sammen ved hash referansene. Endres informasjonen i en blokk vil hash verdien til blokken endres. Dette medfører at alle hash referanser i etterfølgende blokker også endres.



Figur 5 illustrerer hvordan hash referansen lenker blokker sammen på blokkjeden.[85]

[82] Antonopoulos (2015) s. 166.
[83] Figuren er hentet fra Ray (2017).
[84] Bacon mfl. (2018) s. 13.
[85] Inspirasjon for figuren er hentet fra Bacon mfl. (2018) s. 13.

Hash referansen medfører at nodene som verifiserer transaksjoner kan oppdage endringer og forhindre manipulasjon eller forfalskning av dataen.[86] Egenskapen innebærer at informasjon som registreres på blokkjeden aldri kan fjernes eller endres og medfører at opplysningene som ligger på blokkjeden indirekte behandles så lenge blokkjeden eksisterer.[87]

Kort oppsummert hashes data til blokkjeden for å (i) validere at informasjonen ikke har blitt endret (ii) kryptere teksten og (iii) begrense størrelsen på innholdet som skal registreres.

3.7 Konsensusprotokoll

Blokkjedens protokoll angir reglene for hvordan nodene i nettverket skal enes om den nåværende tilstanden til hovedboken ved fravær av et sentralisert kontrollpunkt.[88] Protokollen sikrer at hver node legger til den samme blokken i sin versjon av blokkjeden.[89]

Før nodene aksepterer nye blokker på sin versjon av hovedboken må de først bli generert av en *gruvearbeider*.[90] Gruvearbeiderne gjennomfører prosessen med å samle transaksjoner i blokker. Alle kan bli en gruvearbeider ved å kjøre en spesiell form for fullverdig node. Blokkjeden gir insentiver for å samle transaksjoner i blokker ved å belønne gruvearbeideren for hver gyldig blokk som lages. I tillegg kan gruvearbeideren få et transaksjonsgebyr fra brukeren som overfører en eiendel i retur for at gruvearbeideren prioriterer behandling av deres transaksjon.[91] Belønningene overføres i blokkjedens virtuelle valuta.

Gruvearbeideren må for det første sjekke at transaksjonen er gyldig, det vil si at brukeren har balansen til å kunne overføre eiendelen. I et sentralisert system løses dette ved at en tredjepartstjeneste holder kontroll på hovedboken. I blokkjeden løses problemet ved at gruvearbeideren kalkulerer balansen til brukeren opp mot tidligere transaksjoner på blokkjeden.

For det andre må gruvearbeideren konkurrere mot andre gruvearbeidere om å legge til transaksjonene i en blokk, gjennom en prosess kalt *proof-of-work*.[92] Proof-of-work innebærer at gruvearbeiderne løser et kryptografisk puslespill[93] raskest gjennom prøving og feiling.[94] Det

[86] Drescher (2017) s. 112.
[87] STOA (2019) s. 61.
[88] Ibid. s. 4.
[89] Finck (2019) s. 19.
[90] Ibid. s. 20.
[91] Bacon mfl. (2018) s. 20-21.
[92] Ibid. s. 23.
[93] Puslespillet er lagd ved å sette sammen hash verdien og hash referansen til en blokk. Løsningen er riktig hash verdi for blokken.
[94] Bacon mfl. (2018) s. 24

finnes andre type konsensusprotokoller, men proof-of-work er den vanligste konsensusalgoritmen på Bitcoin- og Ethereum blokkjeden og det redegjøres følgelig for denne.

Formålet med proof-of-work er å sikre mot skadelige aktører som forsøker å ta kontroll over blokkjeden. Ettersom alle kan bli gruvearbeidere, vil det å kunne lage ny blokker gratis kunne overkjøre systemet.[95] Det er dermed svært kostbart å lage nye blokker ettersom man må investere databehandlingsressurser og elektrisitet for å løse puslespillet.[96] Alle gruvearbeiderne bruker ressurser på å løse puslespillet, men bare en vil lykkes først.[97]

Gruvearbeideren som har løst puslespillet kringkaster løsningen til hele nettverket. Nodene verifiserer arbeidet gjennom en enkel databehandlingsprosess og bekrefter at transaksjonen er gyldig. Hvis blokken er gyldig legges den til på noden sin kopi av hovedboken som kringkastes til resten av nettverket. Nodene uttrykker deres aksept av blokken ved å begynne å jobbe på den neste blokken ved å bruke hashen av den aksepterte blokken som hash referansen i den nye blokken.

Latest blocks View more blocks

Number	Hash	Mined	Miner	Transactions	Size
9060074	0xc20bc79e1b3068986d3da3...	26 seconds	0xea674fdde714fd979de3edf...	242	33,699 bytes
9060073	0×696a89047c4fbd4c2ec2a5...	1 minute	0xb2930b35844a230f00e514...	150	28,871 bytes
9060072	0×5f3798b735416a936e1f1cc...	1 minute	0xa3c084ae80a3f039630176...	94	18,984 bytes
9060071	0×954f8f82aa7cd98425e0ec4...	1 minute	0×5a0b54d5dc17e0aadc383d...	212	35,742 bytes
9060070	0xd21d18ec20d5f00be2feef6...	1 minute	0×45a36a8e118c37e4c47ef4a...	0	538 bytes
9060069	0×47d3a44a89d87df12b5a59...	1 minute	0×829bd824b016326a401d08...	166	36,902 bytes

Figur 6 illustrerer blokker registrert på Ethereum blokkjeden; med bla. blokkens hash, gruvearbeiderens (miner) offentlige nøkkel og hvor mange transaksjoner som er samlet i blokken.[98]

3.8 Smart kontrakt

Ethereum-blokkjeden tilrettelegger for programvare på blokkjedens infrastruktur som kan automatisere avtaler mellom aktører i henhold til et sett med instruksjoner innebygget i koden.[99]

[95] Ibid. s. 23.
[96] Ibid. s. 23-24.
[97] Ibid. s. 25
[98] Figuren er et skjermutklipp fra Ethereum-blokkjeden tilgjengelig på: https://www.blockchain.com/eth/block/9060074]
[99] Bacon mfl. (2018) s. 46.

Denne programvaren kalles en *smart kontrakt*. Det er *programvareutviklere* som skriver koden i sekvens og instruksjonene kjøres av *gruvearbeiderne* i bytte for virtuell valuta.

Programvaren utfører automatisk vilkårene i en avtale og utførelsen av avtalen kan ikke stoppes med mindre dette er innebygget i koden.[100] Eksempelvis kan det vises til betaling av husleie. Det er avtalt at husleien betales den 15 hver måned. Denne avtalen skrives av en programvareutvikler i kode på blokkjeden. Når vilkåret oppfylles – det vil si man kommer til den 15 hver måned – frigjøres betalingen fra leietakerens til utleierens offentlige nøkkel.

Det vil ikke redegjøres nærmere om smart kontrakter ettersom de mest relevante problemstillingene er innenfor kontraktsrett, men det er viktig å nevne ettersom *programvareutviklere av smart kontrakter* sin ansvarsrolle må vurderes under GDPR.

[100] Finck (2019) s. 24.

4 Personopplysninger på blokkjeden

4.1 Innledende om GDPRs saklige virkeområde

I dette kapitlet skal det vurderes hvorvidt dataen som behandles på en blokkjede faller innenfor personvernforordningens saklige virkeområde som fremgår av GDPR artikkel 2 nr. 1. Bestemmelsen er inntatt i punkt 2.2.

En blokkjede er et «register» ettersom det er en «strukturert samling av [opplysninger] som er tilgjengelig etter særlige kriterier […]», jf. legaldefinisjonen i artikkel 4 nr. 6, jf. artikkel 2 nr.1.

Legaldefinisjonen av «behandling» fremgår av artikkel 4 nr. 2 og hele bestemmelsen er definert i punkt 2.2. Som nevnt skal definisjonen tolkes vidt og en slik forståelse er avgjørende for blokkjeder som bruker avanserte krypteringsmetoder. Hovedboken oppdateres automatisk ved at nodene og gruvearbeiderne følger protokollen.[101] Overføring og lagring av transaksjoner på blokkjeden er dermed «automatisert behandling», jf. artikkel 4 nr. 2, jf. artikkel 2 nr. 1.

Det problematiske er hvorvidt dataen som behandles på blokkjeden kvalifiseres som «personopplysninger» i henhold til GDPR artikkel 4 nr. 1 ettersom offentlige nøkler og transaksjonsdata som oftest er kryptert.

Personvernforordningen kommer ikke til anvendelse på anonyme opplysninger, som etter fortalepunkt 26 er opplysninger som ikke kan knyttes til en «identifiserbar fysisk person» eller «personopplysninger som har blitt anonymisert på en slik måte at den registrerte ikke lenger kan identifiseres». Motsetningsvis vil pseudonymiserte personopplysninger kvalifiseres som «personopplysninger» da den indirekte identifiseringen av en fysisk person fremdeles er mulig, jf. fortalepunkt 26.

Spørsmålet som skal besvares i dette kapitlet er hvorvidt offentlig nøkler og transaksjonsdata er «personopplysninger» i henhold til GDPR artikkel 4 nr. 1 eller om opplysningene har blitt anonymisert på en slik måte at den registrerte ikke lenger kan identifiseres.

[101] Buocz mfl. (2019) s. 190.

4.2 Behandles det personopplysninger på blokkjeden?

4.2.1 Innledning

Legaldefinisjonen av «personopplysninger» fremgår av GDPR artikkel 4 nr. 1 og hele bestemmelsen er inntatt i punkt 2.2. Artikkel 29-gruppen har i sine retningslinjer om personopplysninger uttalt at definisjonen består av fire kumulative vilkår; personopplysninger kan være «enhver opplysning», opplysningene må være «om» en «fysisk person» og opplysningene må handle om en «identifisert eller identifiserbar fysisk person».[102]

Blokkjedens offentlige nøkkel og transaksjonsdata er «enhver opplysning» i lys av bestemmelsens vide virkeområde.[103] Videre er det klart at offentlige nøkler og transaksjonsdata vil være «om» en «fysisk person».[104] Det problematiske er hvorvidt opplysningene som lagres på blokkjeden handler om en «identifiserbar» fysisk person.

Ordlyden i personverndirektivet artikkel 2 bokstav a er sammenfallende mer GDPR artikkel 4 nr. 1, med unntak av en mer omfattende liste av identifikatorer i GDPR som har sammenheng med den teknologiske utviklingen. Tidligere rettspraksis, Artikkel 29-gruppens uttalelser og øvrige rettskilder er dermed relevante ved tolkningen av vilkåret i GDPR artikkel 4 nr. 1.

I det følgende vil det redegjøres for vilkåret «identifiserbar» i artikkel 4 nr. 1, før vilkåret knyttes opp mot offentlige nøkler og transaksjonsdata som lagres på blokkjeden.

4.2.2 Vilkåret "identifiserbar" opplysning

Ordlyden «identifiserbar» tilsier at det foreligger opplysninger som gjør det mulig å skille en fysisk person fra andre personer. Det presiseres i artikkel 4 nr. 1 at en fysisk person er «identifiserbar» dersom han eller hun «direkte eller indirekte kan identifiseres, særlig ved hjelp av en identifikator».

Ordlyden «direkte […] identifiseres» tilsier at informasjonen klart peker tilbake på individet. Navnet til en fysisk person er den vanligste formen for direkte identifisering.[105] Det er på det rene at personopplysninger som registreres på blokkjeden i klar tekst, for eksempel at Marte

[102] A29 WP Opinion 4/2007, s. 6.
[103] Personopplysninger kan ta hvilken som helst form, eksempelvis alfabetisk, numerisk eller fotografisk, jf. A29 WP Opinion 4/2007, s. 6-7.
[104] Det avgrenses mot opplysninger som gjelder juridiske personer, jf. GDPR fortalepunkt 14.
[105] A29 WP Opinion 4/2007, s. 6-7.

ved overføringen av virtuell valuta til Peder skriver i et notat-område «200 Ether overføres til Peder Ås med adresse Magnus Lagabøtes plass 1» er en personopplysning om en «identifiserbar» fysisk person.

Ordlyden «indirekte […] identifiseres» taler om avledete momenter som kan være gjenstand for identifikasjon. GDPR artikkel 4 nr. 1 viser til eksempler på identifikatorer som kan bidra til identifiseringen, f.eks. navn, identifikasjonsnummer, lokaliseringsopplysninger og en nettidentifikator. I fortalepunkt 30 oppstilles det eksempler på slike nettidentifikatorer, som blant annet IP-adresser. Synspunktet i fortalen om IP-adresser er kodifisering av EU-domstolens uttalelse i Scarlet Extended-dommen[106] hvor domstolen la til grunn at en IP-adresse er en personopplysning fordi den tillater brukeren til å bli «precisely identified».

I Breyer-dommen[107], som gjaldt spørsmål om en dynamisk IP-adresse var en «personopplysning», kom EU-domstolen til at dynamiske IP-adresser er identifikatorer selv om det var internettleverandøren og ikke den behandlingsansvarlige (operatøren av nettsiden som lagret personopplysningene) som satt på tilleggsopplysningene. Avgjørelsen kan tas til inntekt for at opplysningene som muliggjør identifisering trenger ikke å være i hendende på kun en person. Synspunktet er kodifisert i GDPR gjennom ordlyden «eller annen person» i fortalepunkt 26.

I vurderingen om en fysisk person er «identifiserbar», skal det tas hensyn til «alle midler som med rimelighet kan tenkes at den behandlingsansvarlige eller annen person kan ta i bruk for å identifisere vedkommende direkte eller indirekte», jf. fortalepunkt 26. Uttalelsen «med rimelighet» tilsier at det må avgrenses mot uforholdsmessig høye tiltak som må tas i bruk for å identifisere personen.

Det presiseres i fortalepunkt 26 at i vurderingen av hvilke midler som «med rimelighet» kan tenkes å bli tatt i bruk for å identifisere vedkommende «bør det tas hensyn til alle objektive faktorer, f.eks. kostnadene for og tiden som er nødvendig for å foreta identifikasjonen, idet det tas hensyn til teknologien som er tilgjengelig på behandlingstidspunktet, samt den teknologiske utvikling».

[106] Sak C-70/10, avsnitt 51.
[107] Sak C-582/14, avsnitt 49.

I den nevnte Breyer-dommen uttalte domstolen at det kan ikke forventes at midler kan «med rimelighet» tas i bruk hvis de er «prohibited by law or practically impossible on account of the fact that it requires a disproportionate effort in terms of time, cost and man-power, so that the risk of identification appears in reality to be insignificant".[108] Uttalelsen «practically impossible» og «disproportionate effort» kan tas til inntekt for at EU-domstolen har lagt terskelen høyt for å se vekk fra supplerende opplysninger som har mulighet til å identifisere en fysisk person.

Artikkel 29-gruppen gir et eksempel på tidsperspektivet i lys av alle midler som med rimelighet kan tas i bruk for å identifisere en fysisk person.[109] Dersom opplysningene skal lagres i en måned vil identifisering trolig ikke være aktuelt i lys av teknologien tilgjengelig på behandlingstidspunktet. Imidlertid stiller dette seg annerledes dersom opplysningene skal lagres i 10 år og det vil være mest sannsynlig, i lys av den teknologiske utviklingen, å identifisere den fysiske personen om 9,5 år.[110] Opplysningene vil dermed kvalifiseres som personopplysninger på behandlingstidspunktet, selv om det først vil være mulig å identifisere den fysiske personen om 10 år.

Et slikt tidsperspektiv vil være problematisk ved anvendelse av blokkjeder. Egenskapen til blokkjeder medfører at alle transaksjoner registrert i hovedboken siden den første blokken ble lagd vil ligge på en blokkjede i ubestemt tid ettersom det ikke er mulig å endre eller slette opplysningene. Dette taler for at alle opplysninger som registreres på blokkjeden, uavhengig av anonymiseringsmetode, vil være mulig å identifisere en dag som følge av teknologisk utvikling.

I lys av ordlyden i artikkel 4 nr. 1, EU-domstolens avgjørelser, samt veiledningen fra Artikkel 29-gruppen, vil vurderingen av hvorvidt den registrerte er «identifiserbar» på en blokkjede bero på hvorvidt det er mulig å kombinere en offentlig nøkkel eller transaksjonsdata sammen med supplerende data som er i hendende på den aktuelle behandlingsansvarlige eller annen person, og om dette er midler som med rimelighet kan tenkes å bli brukt for å identifisere den registrerte.

[108] Sak C-582/14, avsnitt 46.
[109] A29 WP Opinion 4/2007, s. 15.
[110] Ibid.

4.2.3 Identifiserer en offentlig nøkkel den registrerte?

Det første spørsmålet er om en fysisk person er «identifiserbar» på blokkjeden fordi det er mulig å kombinere en *offentlig nøkkel* med supplerende opplysninger som identifiserer den registrerte, og hvorvidt dette er midler som med rimelighet kan tenkes å bli brukt, jf. artikkel 4 nr. 1.

Offentlige nøkler består av en rekke tilfeldig genererte nummer og tall. Eieren av nøkkelen kan dermed ikke identifiseres direkte på blokkjeden. Imidlertid vil det være mulig å identifisere den reelle eieren av nøkkelen ved bruk av supplerende informasjon. I det følgende vil det vises til ulike måter eieren av den offentlige nøkkelen kan identifiseres på blokkjeden.

For det første vil brukeren av en blokkjede avsløre IP-adressen sin når han eller hun logger seg på blokkjede-nettverket. Brukerens offentlige nøkkel vil dermed kunne knyttes til hennes IP-adresse som ligger registrert hos internettleverandøren, jf. Breyer-dommen.[111] Imidlertid kan brukeren skjule IP-adressen ved å bruke et anonymt kommunikasjonsnettverk, f.eks. Tor.[112]

Videre må brukere som får tilgang til hovedboken via tredjepartstjenester registrere blant annet telefonnummer og epost-adresse for å kunne benytte seg av plattformen. Sammenligner tredjeparten sine lister med brukerens offentlige nøkkel vil brukerens identitet kunne avsløres.

Bacon mfl. (2018) viser til at i tilfeller hvor brukeren betaler for en vare i virtuell valuta vil kjøpmannen kunne lagre den offentlige nøkkelen til kunden og dermed identifisere foretatte transaksjoner fra kundens offentlige nøkkel.[113] Et annet eksempel er hvis brukeren kjøper en sofa og registrerer hjemmeadressen sin i notatfeltet for levering. Imidlertid kan brukeren sikre seg mot slik identifisering og øke sitt personvern ved å generere nye offentlige nøkler og dermed brukernavn, som nevnt i 3.5.1.

Videre vil det være mulig å identifisere brukeren av blokkjeden ved å koble den offentlige nøkkelen opp mot datoen for transaksjonen og betalingssummen. Eksempelvis kan vi se for oss Marte og Peder møtes for en kaffe.[114] Peder ser at Marte betaler for kaffen med Ether. Når transaksjonen registreres på Ethereum-blokkjeden er det mulig for Peder (eller en tredjepart som også observerer kjøpet) å finne tidsstempelet og summen på blokkjeden, og dermed avsløre Martes offentlige nøkkel. Har Marte brukt den samme offentlige nøkkelen for alle transaksjoner

[111] Sak C-582/14.
[112] Buocz mfl. (2019) s. 189.
[113] Bacon mfl. (2018) s. 61.
[114] Eksempelet er hentet fra STOA (2019) s. 23.

hun har overført på blokkjeden vil det være mulig å undersøke alle transaksjoner hun noensinne har foretatt på blokkjeden.

I lys av de ovenstående metodene legges det til grunn at en offentlig nøkkel kan suppleres med tilleggsopplysninger som med rimelighet kan tenkes å bli brukt, jf. artikkel 4 nr. 1. Denne forståelsen har CNIL[115] og EBOF[116] lagt til grunn. I tillegg uttales det i Europaparlamentets studie fra 2019, med henvisning til de førstnevnte institusjonene, at offentlige nøkler som oftest kvalifiserer seg som «personopplysninger» i henhold til GDPR.[117]

En offentlig nøkkel kan dermed ikke ansees som en anonym opplysning, men en pseudonymisert personopplysning som omfattes av reglene i GDPR, jf. artikkel 4 nr. 5, jf. artikkel 2 nr. 1.

4.2.4 Identifiserer transaksjonsdataen den registrerte?

Det neste spørsmålet er om en fysisk person er «identifiserbar» på blokkjeden fordi det er mulig å kombinere *transaksjonsdataen* med supplerende opplysninger som identifiserer den registrerte, og hvorvidt dette er midler som med rimelighet kan tenkes å bli brukt, jf. artikkel 4 nr. 1.

Det er viktig å presisere at transaksjonsdataen ikke nødvendigvis inneholder personopplysninger. Dette må avgjøres konkret i hver behandling. Videre må det avgrenses mot transaksjonsdata som ligger *«off-chain»*, det vil si transaksjonsdata som ikke hashes til blokkjeden, men ligger i hovedboken i form av en hash referanse som viser at informasjonen eksisterer utenfor blokkjeden.

Transaksjonsdataen kan enten lagres på blokkjeden i klar tekst eller bli kryptert eller hashet til blokkjeden. Siden blokkjeden er en offentlig database blir opplysningene som oftest kryptert eller hashet før de legges til på blokkjeden. Som nevnt i punkt 4.2.2 er det på det rene at behandling av transaksjonsdata som registreres på blokkjeden i klar tekst - navnet til mottaker eller andre fysiske personer, telefonnummer, fødselsdato ol. – er «personopplysninger» og faller innenfor GDPRs saklige virkeområde.

[115] Oppsummering av CNILs veileder om blokkjeder (2018), s. 2.
[116] EBOF (2018), s. 19.
[117] STOA (2019) s. 28.

Det første som må vurderes er hvorvidt transaksjonsdata som *krypteres* med en nøkkel kan ansees som «personopplysninger». I Artikkel 29-gruppens veileder om anonymiseringsteknikker understrekes det at kryptering med en hemmelig nøkkel anses som en pseudonymiseringsteknikk[118] Uttalelsen innebærer at transaksjonsdataen som krypteres med en nøkkel og som kan dekrypteres med mottakerens nøkkel er pseudonyme opplysninger ettersom det foreligger supplerende informasjon som kan identifisere den registrerte. Dette gjelder uavhengig av om behandlingsansvarlig har tilgang til den private nøkkelen, jf. Breyer-dommen.[119] Samlet sett innebærer dette at transaksjonsdata kryptert med en nøkkel kan ansees som «personopplysninger», jf. artikkel 4 nr. 1.

Deretter må det vurderes transaksjonsdata som *hashes* til blokkjeden kan ansees som «personopplysninger». Artikkel 29-gruppen uttaler at bruken av en hash funksjon vil ikke automatisk omgjøre personopplysninger til anonyme opplysninger.[120] I veilederen uttales det at «[…] if the range of input values the hash function are known they can be replayed through the hash function in order to derive the correct value for a particular record".[121] Uttalelsen viser til at selv om hashing er en enveis-funksjon, vil det være mulig å koble informasjonen utenom blokkjeden.

Eksempelvis, dersom dokumentet med teksten «Betaling for overføring av hytten Solglimt fra Marte Kirkerud til Peder Ås» kjøres gjennom en hash-funksjon vil det ikke være mulig å gjenopprette teksten. Imidlertid, dersom Ole Vold har kjennskap til dokumentet og teksten, og lurer på hva hytten ble solgt for, kan han kjøre beskjeden gjennom en hash-funksjon og identifisere overføringen ettersom dataen er lik og vil gi en tilsvarende hash-verdi.

Transaksjonsdata med personopplysninger som hashes til blokkjeden kan dermed ansees som «personopplysninger» i henhold til artikkel 4 nr. 1 og omfattes av reglene i GDPR, jf. artikkel 4 nr. 5, jf. artikkel 2 nr. 1.

[118] A29 WP Opinion 05/2014, s. 20.
[119] Sak C-582/14.
[120] A29 WP Opinion 05/2014, s. 20.
[121] Ibid.

5 Identifisering av behandlingsansvarlig

5.1 Innledning

Offentlige nøkler og transaksjonsdata som inneholder personopplysninger som har blitt kryptert eller hashet ansees som personopplysninger i henhold til GPR artikkel 4 nr. 1 og faller dermed innenfor GDPRs saklige virkeområde, jf. artikkel 2 nr. 1.

Dette reiser spørsmålet om hvem som er ansvarlig for behandling av personopplysningene på blokkjeden. I dette kapitelet vil det redegjøres for *hvordan* en behandlingsansvarlig kan identifiseres på blokkjeden, før den juridiske statusen til hver enkelt aktør på blokkjeden vurderes i kapittel seks.

Legaldefinisjonen av behandlingsansvarlig fremgår av GDPR artikkel 4 nr. 7 og bestemmelsen er inntatt i punkt 2.3. Artikkel 29-gruppen har uttalt i sine retningslinjer om behandlingsansvarlig og databehandler at definisjonen består av tre elementer.[122] For det første må det være tale om en «fysisk eller juridisk person, en offentlig myndighet, en institusjon eller ethvert organ». For det andre må det identifiseres hvem som «bestemmer formålet med behandlingen av personopplysninger og hvilke midler som skal benyttes». Og til slutt må det vurderes hvorvidt aktøren har kontroll over personopplysningene «alene eller sammen med andre». Drøftelsen disponeres ut fra disse tre elementene.

GDPR artikkel 4 nr. 7 er sammenfallende med definisjonen i personverndirektivet artikkel 2 bokstav b. Dermed er rettspraksis, veiledninger og øvrige rettskilder fremdeles relevante ved tolkningen av vilkårene i GDPR artikkel 4 nr. 7.

I det følgende skal det redegjøres for de tre kumulative vilkårene i artikkel 4 nr. 7 og knytte de opp mot blokkjedens elementer. I tilfeller hvor *databehandler* nevnes vises det til legaldefinisjonen av databehandler inntatt i punkt 2.3.

[122] A29 WP Opinion 1/2010, s. 7.

5.2 Vilkårene for identifisering av behandlingsansvarlig

5.2.1 Hvem kan være behandlingsansvarlig på blokkjeden?

For det første må det klargjøres *hvem* som kan være behandlingsansvarlig. Behandlingsansvarlig må være en «fysisk eller juridisk person, en offentlig myndighet, en institusjon eller ethvert organ». Ordlyden favner vidt og sikrer at enhver innflytelsesrik aktør som behandler personopplysninger må forholde seg til reglene og prinsippene i forordningen.

Artikkel 29-gruppen uttaler at forståelsen av dette elementet skal sikre «effective application» av personvernlovgivningen.[123] Uttalelsen må sees i lys av EU-domstolens uttalelse i den nevnte Google Spain-dommen[124] om at definisjonen *behandlingsansvarlig* skal tolkes vidt for å sikre en «effective and complete protection of data subjects».

Det er uomtvistet at aktørene på blokkjeden - grunnleggeren, programvareutviklere, noder, gruvearbeidere og brukere av blokkjeden - faller inn under den vide ordlyden av «fysiske eller juridiske personer».

5.2.2 Hvem bestemmer formålet med behandlingen og hvilke midler som skal benyttes?

Videre må det identifiseres hvem som «bestemmer formålet med behandlingen av personopplysninger og hvilke midler som skal benyttes».

Ordlyden «bestemmer» viser til aktøren som har den reelle innflytelsen over formålet med og midlene som skal benyttes i behandlingen av personopplysninger. Ordlyden må forstås i lys av ansvarsprinsippet i artikkel 5 nr. 2 ettersom aktøren som avgjør hvorfor personopplysninger skal behandles er også det naturlige subjektet å identifisere som ansvarlig for behandlingen.

Artikkel 29-gruppen uttaler at ordlyden «bestemmer» skal forstås «functional, in the sense that it is intended to allocate responsibilities where the factual influence is, and thus based on a factual rather than a formal analysis".[125] Uttalelsen innebærer at det må vurderes hvor den faktiske innflytelsen over avgjørelsen ligger og ikke hva som er formelt avgjort eller definert.

[123] A29 WP Opinion 1/2010, s. 15.
[124] Sak C-131/12, avsnitt 34.
[125] A29 WP Opinion 1/2010, s. 1.

Formålet er å hindre at aktører som har faktisk innflytelse over behandlingen av personopplysninger, omgår reglene ved å definere sin ansvarsrolle slik de selv ønsker, og dermed unngår forpliktelsene som følger av behandlingsansvaret.

Ordlyden «bestemmer» i artikkel 4 nr. 7 og Artikkel 29-gruppens veileder tilsier dermed at det må vurderes hvilke aktører som har den *faktiske innflytelsen* over formålet med og midlene som skal benyttes i den konkrete behandlingen. Hvor den faktiske innflytelsen ligger kan imidlertid være problematisk å stadfeste blant aktørene på en blokkjede ettersom den sentraliserte myndigheten er fjernet og kontrollen er fordelt likt over hele nettverket.

Videre må det vurderes hva som omfattes av «formålet» og «midler» ved behandlingen av offentlige nøkler og transaksjonsdata. Bacon mfl. (2018) viser til at formålet og midlene ved behandling av personopplysninger på en blokkjede kan vurderes ut fra to interessante perspektiv; enten makronivå eller mikronivå.[126] Et makronivå perspektiv innebærer at man ser på formålet og midlene som brukes ved anvendelse av blokkjeden i sin helhet, mens fra et mikronivå perspektiv ser man på formålet og midlene som brukes for den individuelle transaksjonen. I det følgende skal vilkårene sees i lys av disse to perspektivene.

Ordlyden «formålet» tilsier motivasjonen bak aktørenes ønske om å behandle de konkrete personopplysningene. Artikkel 29-gruppen understreker at vurderingen beror på *hvorfor* personopplysningene skal behandles.[127] Fra et makronivå perspektiv er «formålet» med behandlingen av den offentlige nøkkelen og transaksjonsdataen å tilby selve tjenesten, det vil si tilrettelegge for at Marte kan bruke blokkjeden for å overføre en eiendel til Peder.[128] Fra et mikronivå perspektiv er «formålet» med behandlingen av den offentlige nøkkelen og transaksjonsdataen å registrere en individuell transaksjon på blokkjeden.[129]

Ordlyden «midler» tilsier hvilke hjelpemidler som skal benyttes for å oppnå formålet med behandlingen. Artikkel 29-gruppen avklarer at vilkåret «midler» ikke kun refererer til tekniske og organisatoriske måter å behandle personopplysninger på, men også til hvem som bestemmer *hvordan* personopplysningene skal behandles.[130] Fra et makronivå perspektiv innebærer «midler» hvilken programvare og maskinvare nodene velger å bruke for å finne, samle og

[126] Bacon mfl. (2018) s. 64.
[127] A29 WP Opinion 1/2010, s. 13.
[128] Bacon mfl. (2018) s. 64.
[129] Ibid.
[130] A29 WP Opinion 1/2010, s. 14.

verifisere transaksjoner i blokkjede nettverket.[131] Fra et mikronivå perspektiv er «midler» brukerens valg av blokkjede plattformen, det vil si Martes avgjørelse om å bruke en blokkjede fremfor en annen løsning, eksempelvis en nettbank, for å kunne overføre en eiendel til Peder.[132]

En naturlig forståelse av sammenhengen mellom vilkårene i artikkel 4 nr. 7 tilsier at aktøren må bestemme formålet *og* midlene med behandlingen for å kunne kvalifiseres som behandlingsansvarlig. Imidlertid har Artikkel 29-gruppen presisert at «while determining the purpose of the processing would in any case trigger the qualification as controller, determining the means would imply control only when determination concerns the essential elements of the means" [133] (forfatterens understrekninger). Uttrykket "in any case" tilsier at en hvilken som helst påvirkning over formålet med behandlingen utløser behandlingsansvar. Når det gjelder hva som omfattes av «essential elements of the means» trekker Artikkel 29-gruppen frem eksempler som hvilke opplysninger som skal behandles, hvilke tredjeparter som skal få tilgang til opplysningene og når opplysningene skal slettes.[134]

Følgelig er det formålsvilkåret som er det primære vilkåret ved identifisering av behandlingsansvarlig. Dette innebærer at en aktør på blokkjeden som har en hvilken som helst *faktisk innflytelse* over *formålet* med behandlingen vil kunne kvalifiseres som behandlingsansvarlig. Vedrørende *midlene* som benyttes i behandlingen skiller Artikkel 29-gruppen mellom tekniske og organisatoriske midler som kan delegeres videre til databehandler (f.eks. valg av programvare, maskinvare ol.) og avgjørelser som er forbeholdt behandlingsansvarlig (f.eks. hvilke personopplysninger som skal behandles eller hvor lenge personopplysningene skal lagres).[135]

Samlet sett gir artikkel 4 nr. 7 og Artikkel 29-gruppens veileder uttrykk for at vurderingen som må foretas for å identifisere behandlingsansvarlig på en blokkjede beror på en vurdering av hvor den faktiske innflytelsen over formålet med behandlingen ligger og om aktøren avgjør midler som er forbeholdt behandlingsansvarlig, eller om aktøren kun avgjør tekniske og organisatoriske spørsmål knyttet til behandlingen. I sistnevnte tilfelle vil aktøren kunne defineres som databehandler. Ansvarsforholdet mellom eventuelle behandlingsansvarlige og databehandlere på blokkjeden vil behandles nærmere i 6.3.2.

[131] Bacon mfl. (2018), s. 64.
[132] Ibid.
[133] A29 WP Opinion 1/2010, side 14.
[134] Ibid.
[135] Ibid.

5.2.3 Foreligger det felles behandlingsansvar?

Til slutt må det vurderes hvordan aktørene som identifiseres som behandlingsansvarlige på blokkjeden kan være felles behandlingsansvarlige. Legaldefinisjonen av felles behandlingsansvar fremgår av GDPR artikkel 26 og bestemmelsen er inntatt i punkt 2.3.

Felles behandlingsansvar var ikke definert i personverndirektivet, men fremgikk indirekte av ordlyden i personverndirektivets artikkel 2 (2) «alene eller sammen med andre» som tilsvarer ordlyden i GDPR artikkel 4 nr. 7. Tidligere rettspraksis, Artikkel-29 gruppens uttalelser og øvrige rettskilder er dermed relevante ved tolkningen av GDPR artikkel 26, jf. artikkel 4 nr. 7.

Artikkel 26 oppstiller tre kumulative vilkår for at det skal foreligge felles behandlingsansvar. Drøftelsen disponeres ut fra disse tre vilkårene.

For det første må det foreligge «to eller flere behandlingsansvarlige». En blokkjede består av et omfattende nettverk av aktører som behandler offentlige nøkler og transaksjonsdata. Det vil dermed kunne være flere aktører som har faktisk innflytelse over formålet med behandlingen av personopplysningene.

For det andre må to eller flere behandlingsansvarlige «i fellesskap» fastsette formålet med og midlene for behandlingen. Ordlyden «i fellesskap» tilsier at flere behandlingsansvarlige har tilsvarende faktisk innflytelse over formålet med behandlingen og hvilke midler som skal benyttes i den konkrete behandlingen. Artikkel 29-gruppen avklarte imidlertid at felles behandlingsansvar «may take different forms and does not need to be equally shared»[136]. Uttalelsen tilsier at felles behandlingsansvar foreligger mellom flere aktører på blokkjeden selv om graden av innflytelse over formålet og midlene som skal benyttes varierer.

En slik forståelse ble lagt til grunn i Wirtschaftsakademie Schleswig – Holstein-dommen[137] (heretter «WSH-dommen») hvor EU-domstolen uttalte at felles behandlingsansvar ikke trenger å innebære «equal responsibility» mellom de behandlingsansvarlige og understreket at partene «may be involved at different stages of that processing of personal data and to different degrees» uten at det avgrenset mot felles behandlingsansvar.[138]

[136] A29 WP Opinion 1/2010, s. 19.
[137] Sak C-210/16.
[138] Ibid. avsnitt 43.

EU-domstolens uttalelse i WSH-dommen og Artikkel 29-gruppens veileder tilsier dermed at det kan foreligge ulikt ansvar i ulike stadier av behandlingen mellom felles behandlingsansvarlige. En slik fordeling må sees i lys av at personopplysninger behandles i stadig mer komplekse nettverk av flere aktører.

Aktørene på blokkjeden behandler offentlige nøkler og transaksjonsdata i ulike grader og stadier. Spørsmålet er dermed hvilken grad av faktisk innflytelse over formålet og midlene som kreves for å bli ansett som felles behandlingsansvarlig på en blokkjede.

En naturlig forståelse av GDPR artikkel 26 tilsier at felles behandlingsansvar foreligger når to eller flere behandlingsansvarlige bestemmer både formålet med *og* midlene i fellesskap. Imidlertid har Artikkel-29 gruppen uttalt at felles behandlingsansvar foreligger selv om aktørene «shar[es] only purposes or means».[139] Dette innebærer at aktørene på blokkjeden kan ansees som felles behandlingsansvarlige selv om de kun bestemmer formålet med behandlingen i fellesskap, eller kun hvilke midler som skal benyttes i felleskap.

I Jehovas Witness-dommen[140] kom EU-domstolen frem til at et trossamfunn kunne ansees som felles behandlingsansvarlig med sine medlemmer som gikk fra dør til dør og samlet inn personopplysninger i sammenheng med forkynnelse av troen. Domstolen begrunnet avgjørelsen i at forkynnelse av troen var organisert og koordinert på en måte som var oppfordret av trossamfunnet.[141] EU-domstolen uttalte at aktøren som «excerts influence over the processing of personal data, for his own purposes, and who participates, as a result, in the determination of the purposes and means of processing» kunne ansees som felles behandlingsansvarlig.[142] (forfatterens understrekninger).

Avgjørelsen kan tas til inntekt for at terskelen for å identifiseres som felles behandlingsansvarlig er at aktøren har *påvirkende innflytelse* over behandlingen av personopplysningene for *sine egne formål*. Oppfattelsen til EU-domstolen ble bekreftet i den nylig avsagte Fashion ID-dommen.[143]

Overført til en blokkjede vil alle aktørene som velger å delta i nettverket kunne kvalifiseres som felles behandlingsansvarlige for behandlingen av personopplysningene. Dette gjelder selv om

[139] A29 WP Opinion 1/2010, s. 19.
[140] Sak C-25/17.
[141] Ibid. avsnitt 71.
[142] Ibid. avsnitt 68.
[143] Sak C-40/17, avsnitt 68.

aktørene har begrenset kontroll over formålet og ingen innflytelse over hvilke midler som skal benyttes for å behandle de offentlige nøklene og transaksjonsdataen. Hvorvidt aktører på blokkjeden er felles behandlingsansvarlige vil det redegjøres for i punkt 6.3.1.

Til slutt kreves det at de behandlingsansvarlige formaliserer samarbeidet gjennom en «ordning seg imellom», jf. artikkel 26 nr. 1 annen setning. Ordlyden «ordning seg imellom» viser til at det må foreligge en avtale mellom de behandlingsansvarlige. Ordlyden «ordning» tilsier at det ikke er krav til en formell avtale. Problematikken knyttet til gjennomføring av en slik ordning diskuteres nærmere i punkt 6.3.1.

6 Aktørenes ansvarsrolle på blokkjeden

6.1 Innledende om analysens utgangspunkt

I dette kapittelet vil den juridiske statusen til aktørene på blokkjeden vurderes; herunder *grunnleggeren, programvareutviklere, brukere, noder, gruvearbeidere.* Det vil i tillegg knyttes noen bemerkninger vedrørende statusen til *programvareutviklere av smart kontrakter* og *tilbydere av veksling- og oppbevaringstjenester for virtuell valuta*. Formålet er å identifisere behandlingsansvarlige, og eventuelt databehandlere, på blokkjeden. Avslutningsvis vil problematikk knyttet til avtaleforhold mellom identifiserte aktører på blokkjeden kort forklares.

Analysen vil ta utgangspunkt i hvem bestemmer *formålet* med behandlingen og hvilke *midler* som skal benyttes, jf. artikkel 4 nr. 7. Bacon mfl. (2018) argumenterer for at det er hensiktsmessig å foreta identifiseringen av behandlingsansvarlig fra et mikronivå perspektiv siden personvernlovgivningen retter seg mot individuelle behandlinger av personopplysninger.[144] Et tilsvarende perspektiv legges til grunn i denne vurderingen.

Vurderingen beror dermed på hvem som har den *faktiske innflytelsen* over *formålet* med behandlingen av personopplysninger i den individuelle overføringen og om aktøren avgjør *midler* som er forbeholdt behandlingsansvarlig, eller kun avgjør tekniske og organisatoriske spørsmål som tilfaller databehandler, jf. punkt 5.2.2.

6.2 Identifisering av ansvarsroller

6.2.1 Rollen til grunnleggeren og programvareutviklere

Det første som må vurderes er om *grunnleggeren(e)* av blokkjeden er behandlingsansvarlig for personopplysningene som registreres på den konkrete blokkjeden. For å belyse vurderingen kan grunnleggeren av Ethereum-blokkjeden – programmereren Vitalik Buterin - brukes som et eksempel.

Buterin utformet Ethereum-blokkjeden for at den skulle tjene som infrastruktur for direkte kontakt mellom to aktører i et nettverk, samt tilrettelegge for smart kontrakter. Buterin bestemte

[144] Bacon mfl. (2018) s. 65.

dermed hvilket formål blokkjeden skulle tjene og utviklet protokollen i henhold til formålet. Dette taler for at Buterin er behandlingsansvarlig ettersom han har faktisk innflytelse over formålet med blokkjeden og hvordan formålet skal oppnås (i henhold til protokollen).

Imidlertid utviklet Buterin kun et desentralisert verktøy tilgjengelig for alle. I en rapport for EBOF uttales det at "[h]olding developers accountable under these circumstances would be like holding Tim Berners-Lee accountable for everything that happens on the world wide web".[145] At grunnleggeren av en blokkjede skal stilles ansvarlig for personopplysninger som registreres på blokkjeden vil være uforholdsmessig ettersom grunnleggeren ikke har faktisk innflytelse over hvorfor de offentlige nøklene og transaksjonsdataen behandles i den individuelle overføringen. Grunnleggeren(e) av en blokkjede kan dermed ikke ansees som behandlingsansvarlig for personopplysninger som registreres på sin konkrete blokkjede.

En tilsvarende forståelse må legges til grunn for *programvareutviklere.* Programvareutviklere vedlikeholder og oppdaterer protokollen, men bestemmer ikke hvorfor de offentlige nøklene og transaksjonsdataen behandles i det konkrete tilfellet. I Europaparlamentets studie fra 2019 uttales det at programvareutviklere kun gjør tilgjengelig en infrastruktur som aktørene i nettverket kan bruke for å realisere sine formål og har dermed ingen faktisk innflytelse over formålet med behandlingen.[146] Dette tilsier at programvareutviklerne heller ikke kan ansees som behandlingsansvarlige.

Videre er det opp til nodene og gruvearbeiderne å avgjøre hvorvidt de ønsker å godta programvareoppdateringene. Programvareutviklerne har dermed ingen faktisk innflytelse over hvilken programvare som godtas eller maskinvare nodene og gruvearbeiderne anvender for innsamlingen og valideringen av transaksjonen på blokkjeden.

Programvareutviklere er følgelig aktører på blokkjeden som vedlikeholder og oppdaterer verktøyet skapt av grunnleggeren, men bestemmer ikke hvorfor eller hvordan verktøyet skal benyttes. Programvareutviklere kan dermed ikke ansees som behandlingsansvarlige eller databehandlere for personopplysningene på blokkjeden.

Annerledes vil det imidlertid kunne stille seg for *programvareutviklere av smart kontrakter*. I Europaparlamentets studie fra 2019, med henvisning til CNIL, uttales det at

[145] EBOF (2018) s. 18.
[146] STOA (2019) s. 46.

programvareutvikleren av smart kontrakten kan ansees om en «simple external provider» i samsvar med programvareutviklere av protokollen, men dersom programvareutvikleren «actively participate» i behandlingen av personopplysninger kan de ansees som databehandler eller felles behandlingsansvarlig avhengig av deres faktiske innflytelse over formålet behandlingen.[147] Dette må vurderes konkret i de individuelle behandlingene av personopplysninger.

6.2.2 Rollen til brukerne av blokkjeden

Brukere av blokkjeder initierer transaksjoner mellom sin offentlige nøkkel og en annen offentlig nøkkel. Mottakerens offentlige nøkkel kan enten tilhøre brukeren eller en annen bruker av blokkjeden.

Etter GDPR artikkel 2 nr. 2 bokstav b kommer ikke personvernforordningen til anvendelse ved behandling av personopplysninger som utføres av en «fysisk person som ledd i rent personlige eller familiemessige aktiviteter».Det første som må avklares er hvorvidt brukerens anvendelse av en blokkjede ansees som behandling av personopplysninger som ledd i «rent personlige eller familiemessige aktiviteter». Bestemmelsen viderefører personverndirektivet artikkel 3 og derfor er tidligere praksis fra EU-domstolen og øvrige rettskilder relevante ved tolkningen av GDPR artikkel 2 nr. 2.

Ordlyden «rent personlige eller familiemessige aktiviteter» tilsier at den fysiske personen ikke har noen kommersiell interesse i behandlingen av personopplysninger. Fortalepunkt 18 presiserer at forordningen gjelder kun ved behandling av personopplysninger som utføres i forbindelse med «yrkes- eller forretningsvirksomhet».

Ryneš-dommen[148] gjaldt spørsmål hvorvidt privat kameraovervåkning som filmet personer som passerte områder i nærheten av huset falt innenfor unntaket for rent personlige eller familiemessige aktiviteter. Bildene ble lagret på en harddisk. EU-domstolen kom frem til at tilfellet ikke falt innenfor unntaket og understreket at unntaket skal tolkes «narrowly» i lys av ordlyden «rent» personlige eller familiemessige aktiviteter.[149] Avgjørelsen tas til inntekt for at unntaket skal tolkes snevert og det foreligger en høy terskel for at noe er «rent» personlige eller

[147] STOA (2019) s. 44, jf. CNILs veileder om blokkjeder (2018) s. 2.
[148] Sak C-212/13, avsnitt 13.
[149] Ibid. avsnitt 30.

familiemessige aktiviteter. I den nylig avsagte Sergejs Buivids-dommen[150] fra 2019 bekreftet domstolen behovet for å tolke unntaket strengt.

Det er på det rene at GDPR kommer til anvendelse når brukeren registrerer personopplysninger på blokkjeden som relaterer seg til «yrkes- eller forretningsvirksomhet» eller når brukeren er en juridisk person som registrerer personopplysninger på blokkjeden. En slik forståelse har blitt lagt til grunn av blant annet CNIL.[151]

I tillegg uttaler CNIL at fysiske personer som registrerer personopplysninger på blokkjeden som ikke relaterer seg til «yrkes- eller forretningsvirksomhet» er ikke behandlingsansvarlige i henhold til GDPR artikkel 2.[152] Dette er imidlertid ikke helt klart. I Europaparlamentets studie fra 2019 presiseres det at det må skilles mellom to ulike typetilfeller hvor brukeren behandler personopplysninger som ikke er knyttet til «yrkes- eller forretningsvirksomhet», men som likevel *kan* omfattes av GDPR.[153] Det vil i det følgende redegjøres for typetilfellene.

Det første tilfellet er når en bruker overfører en eiendel til *sin egen brukerkonto*. I denne overføringen registrerer brukeren sine egne offentlige nøkler, samt transaksjonsdata. Det forutsettes at det ikke foreligger personopplysninger om andre fysiske personer i transaksjonsdataen. Dersom GDPR kommer til anvendelse på slike tilfeller vil brukeren være både behandlingsansvarlig og den registrerte. Den registrertes rettigheter vil i slike tilfeller ikke ha noen selvstendig betydning. Eksempelvis vil den registrertes rett til informasjon fra behandlingsansvarlig i henhold til GDPR artikkel 13 og 14 ikke ha selvstendig betydning hvor den registrerte selv sitter på informasjonen.[154] Det er dermed nærliggende å anta at tilfeller hvor brukeren initierer en transaksjon til sin *egen brukerkonto* ikke omfattes av GDPR.

Det neste tilfellet er når en bruker overfører en eiendel til en *annen brukers brukerkonto* på blokkjeden for sitt eget formål og uten kommersiell interesse knyttet til behandlingen. Det kan trekkes paralleller til publisering av personopplysninger tilhørende en annen på åpne sosiale nettverk og på en blokkjede. Fortalepunkt 18 viser til at «aktiviteter på sosiale nettverk» faller inn under unntaket. Dette taler for at unntaket kommer til anvendelse på typetilfellet.

[150] Sak C-345/17, avsnitt 43.
[151] CNILs veileder om blokkjeder (2018) s.1.
[152] Ibid. s. 2.
[153] STOA (2019) s. 48.
[154] Buocz mfl. (2019) s. 194.

Imidlertid har Artikkel 29-gruppen presisert at brukere av sosiale nettverk som laster opp personopplysninger om tredjeparter er behandlingsansvarlige sammen med leverandøren av det sosiale nettverket.[155] Artikkel 29-gruppens uttalelse må sees i lys av EU-domstolens presisering av unntakets rekkevidde.

Bodil Lindqvist-dommen[156] gjaldt en katolsk lærer som opprettet en hjemmeside for medlemmene i menigheten og publiserte personopplysninger om 18 kollegaer på siden, som blant annet deres navn, stilling i menigheten, telefonnummer og hobbyer. EU-domstolen uttalte at personlige eller familiemessige aktiviteter omfatter ikke behandling av personopplysninger «consisting in publication on the internet so that this data are made accessible to an indefinite number of people».[157] (forfatterens understrekninger)

Uttalelsen i Bodil Lindqvist-dommen ble fulgt opp i blant annet Satamedia-dommen[158] hvor EU-domstolen understreket at unntaket «clearly does not apply» i tilfeller hvor hensikten er å gjøre den innsamlede dataen tilgjengelig for et ubegrenset antall mennesker. Avgjørelsene kan tas til inntekt for at behandling av personopplysninger som når ut til et *ubegrenset antall mennesker* omfattes ikke av unntaket i GDPR artikkel 2 nr. 2 bokstav b.

I Bodil Lindqvist-dommen ble personopplysningene om hennes kollegaer publisert i klar tekst på hjemmesiden. På blokkjeden er personopplysningene enten kryptert eller hashet og det må en viss innsats til for å identifisere personen bak en offentlig nøkkel eller hvem som nevnes i transaksjonsdataen. Dette kan tale for at dommen ikke har overføringsverdi til typetilfellet. Imidlertid kvalifiserer slike opplysninger seg som «personopplysninger» under GDPR som presentert i punkt 4.2.3 og 4.2.4. Dommen har følgelig overføringsverdi.

Det sentrale ved vurderingen er dermed om brukerens anvendelse av blokkjeden medfører at personopplysningene når ut til et *ubegrenset antall mennesker*. I dette konkrete typetilfellet vil brukerens anvendelse av blokkjeden medføre at personopplysninger til en annen fysisk person registreres på hovedboken. Alle som laster ned programvaren har tilgang til hovedboken, og i tillegg har andre personer som ikke laster ned blokkjeden tilgang til informasjonen gjennom tredjepartstjenester. Personopplysningene distribueres dermed til et ubegrenset antall mennesker. Typetilfellet faller innenfor kjerneområdet for hva EU-domstolen uttaler ikke

[155] WP A29 Opinion 1/2010, s. 21.
[156] Sak C-101/01, avsnitt 12-13.
[157] Ibid. avsnitt 47.
[158] Sak C-73/07, avsnitt 44.

omfattes av unntaket. Brukerens anvendelse av blokkjeden ansees dermed ikke som behandling av personopplysninger som ledd i «rent personlige eller familiemessige aktiviteter» i henhold til artikkel 2 nr. 2 bokstav b.

GDPR kommer følgelig til anvendelse på tilfeller hvor brukeren initierer en transaksjon til *en annens brukerkonto.* Det må dermed vurderes om brukeren kan ansees som behandlingsansvarlig for personopplysningene som registreres på blokkjeden, jf. GDPR artikkel 4 nr. 7.

Brukeren bestemmer «formålet» med behandlingen av den offentlige nøkkelen og transaksjondataen ettersom opplysningene behandles for å kunne endre eierforhold på blokkjeden. Videre bestemmer brukeren «midl[et]» - blokkjede-plattformen - som skal anvendes for å kunne oppnå formålet med behandlingen av personopplysningene. Dette taler for at brukeren er behandlingsansvarlig for personopplysninger som registreres på blokkjeden.

At brukeren ikke har faktisk innflytelse over hvilken programvare nodene og gruvearbeiderne kjører er uten betydning da det avgjørende spørsmålet er hvor den faktiske innflytelsen over formålet med behandlingen ligger. Valg av programvare og maskinvare er tekniske og organisatoriske spørsmål som kan delegeres videre til databehandler, jf. punkt 5.2.2.

Den tidligere nevnte WSH-dommen[159] gjaldt spørsmål om administratoren av en Facebook-side kunne ansees som felles behandlingsansvarlig med Facebook. Administratoren var en tysk privatskole som brukte Facebook-siden for å markedsføre privat undervisning. Når en bruker besøkte siden ble en informasjonskapsel som samlet personopplysninger plassert på brukerens datamaskin.[160] Formålet med behandlingen fra Facebook sin side var å optimalisere målrettet reklame på plattformen, mens administratoren innhentet statistikk produsert av Facebook for å administrere markedsføringen av skolen.

EU-domstolen kom frem til at privatskolen var behandlingsansvarlig sammen med Facebook og begrunnet avgjørelsen blant annet med at «[…] the administrator of a fan page hosted on Facebook, by creating such a page, gives Facebook the oppurtunity to place cookies on the computer or other device of a person visiting its fan page […].»[161] (forfatterens understrekning). EU-domstolen la vekt på at administratoren kunne påvirke og dermed bidro til behandling av

[159] Sak C-210/16, avsnitt 25.
[160] Ibid. avsnitt 33.
[161] Ibid. avsnitt 35.

personopplysninger ved å definere enkelte parametere og bestemme hvilke kategorier av personopplysninger de ønsket at Facebook skulle behandle for deres egne formål, eksempelvis alder, kjønn, sivilstatus, yrke ol.[162] Avgjørelsen kan tas til inntekt for at det avgjørende er om aktøren velger plattformen selv og kan dermed påvirke behandlingen av personopplysninger.

Dommen har overføringsverdi til en brukers anvendelse av blokkjeden ettersom de velger blokkjeden som plattform og påvirker dermed behandlingen av personopplysninger. Imidlertid argumenterer Buocz mfl. (2019) at dommen ikke har overføringsverdi til brukerens valg av blokkjeder ettersom brukeren ikke har påvirkende innflytelse over hvor lenge personopplysningene lagres, hvilke tredjeparter som har tilgang til informasjonen og når informasjonen slettes.[163]

Motsetningsvis hevder Bacon mfl. (2018) at brukeren av en blokkjede kan være behandlingsansvarlig og sammenligner forholdet til skytjenester.[164] En kunde som benytter en skytjeneste aksepterer betingelsene og de tekniske modifiseringene til leverandøren.[165] Kunden har mulighet til å velge andre skytjenesteleverandører med andre betingelser og tekniske modifiseringer, og er dermed ansvarlig for deres valg av den konkrete skytjenesten.

En slik forståelse fremgår av WSH-dommen[166] hvor EU-domstolen uttalte at «the fact that an administrator of a fan page uses the platform provided by Facebook in order to benefit from the associated services cannot exempt it from compliance with its obligations concerning the protection of personal data". Uttalelsen kan tas til inntekt for at hvor brukeren selv velger og godtar platformens betingelser er de naturlige aktører å identifisere som behandlingsansvarlige.

Samlet gir artikkel 4 nr. 7, Artikkel 29-gruppens veiledere og WSH-dommen uttrykk for at brukeren er ansvarlig for personopplysningene vedrørende en annen fysisk person ettersom brukeren velger å benytte seg av en blokkjede for å oppnå formålet med behandlingen. Følgelig har brukeren valgt «formålet» med behandlingen og hvilke «midler» som skal benyttes og *kan* dermed identifiseres som behandlingsansvarlig i henhold til GDPR artikkel 4 nr. 7.

Dersom brukere ansees som behandlingsansvarlige oppstår det spørsmål knyttet til etablering av avtaleforhold mellom aktørene. Dette vil det redegjøres for i punkt 6.3.1.

[162] Ibid. avsnitt 36-37.
[163] Buocz mfl. (2019) s. 195.
[164] Bacon mfl. (2018) s. 69.
[165] Ibid.
[166] Sak C-210/16, avsnitt 40.

6.2.3 Rollen til noder

Noder velger hvilken funksjon de ønsker å ha i nettverket, og kan validere transaksjoner og påvirke utviklingen av blokkjeden ved å akseptere eller avslå programvareoppdateringer. Dette tilsier at noder har faktisk innflytelse over behandlingen av personopplysninger på blokkjeden.

Imidlertid har ikke noder faktisk innflytelse over *hvorfor* behandlingen av offentlige nøkler og transaksjonsdata skal gjennomføres i den individuelle transaksjonen. EBOF viser til at nodene kjører programvaren og følger protokollen kun for å bidra med nettverkets stabilitet og/eller få direkte tilgang til informasjonen på hovedboken.[167] Dette tilsier at noder er fastlåst til protokollen og bestemmer ikke hvorfor eller hvordan personopplysningene behandles.

Selv om noder velger å kjøre den konkrete programvaren og velger individuelt hvilken maskinvare som skal benyttes for å validere en transaksjon, har de ikke mulighet til å endre formålet med blokkjeden og reglene i protokollen. Nodene kan velge å avslå programvareoppdateringer, men dette vil føre til opprettelse av en ny blokkjede, uavhengig av den konkrete transaksjonen på den opprinnelige blokkjeden.

Noder som validerer transaksjoner kan dermed ikke ansees som behandlingsansvarlige for personopplysningene som registreres på blokkjeden ettersom de ikke har faktisk innflytelse over *hvorfor* de offentlige nøklene og transaksjonsdataen behandles eller *hvordan* de skal behandles da dette fremgår av reglene i protokollen som de ikke har faktisk innflytelse over.

Spørsmålet er dermed om noder kan ansees som databehandlere som behandler «på vegne» av behandlingsansvarlig, jf. artikkel 4 nr. 8. Det forutsettes for den videre drøftelsen at brukeren av blokkjeden er behandlingsansvarlig.

Skullerud mfl. (2018) uttaler at databehandleren kjennetegnes ved at vedkommende «ikke ville ha hatt faktisk tilgang til de aktuelle personopplysningene uten tjenesteoppdraget».[168] Overført til nodene på blokkjeden vil heller ikke de hatt tilgang til de offentlige nøklene og transaksjonsdataen uten at brukeren initierer transaksjonen til nettverket.

Videre sammenligner Bacon mfl. (2018) nodenes behandling av transaksjoner på vegne av brukeren med leverandører av skytjenester.[169] En skytjenesteleverandør ansees som

[167] EBOF (2018) s. 18.
[168] Skullerud mfl. (2018) s. 62.
[169] Bacon mfl. (2018) s. 71.

databehandler for personopplysningene som behandles på vegne av kunden. I likhet med kunden av en skytjeneste, bestemmer brukeren hvilke personopplysninger som skal behandles på blokkjeden. Og nodene, i likhet med leverandøren av skytjenesten, stiller tilgjengelig databehandlingsressurser for brukeren.[170]

Samlet sett tilsier ovenstående at noder kan ansees som databehandlere ettersom de stiller databehandlingsressurser tilgjengelig for brukeren og validerer transaksjonen, og behandler dermed personopplysningene «på vegne» av brukeren, jf. GDPR artikkel 4 nr. 8. Ansees noder som databehandlere oppstår det spørsmål knyttet til avtaleforhold med behandlingsansvarlig. Dette vil det redegjøres for i punkt 6.3.2.

Det er imidlertid viktig å skille mellom noder som behandler personopplysninger på vegne av brukerne og noder som tar en mer aktiv rolle i behandlingen av personopplysninger på blokkjeden.[171] Dette må sees i lys av at det avgjørende er hvor den faktiske innflytelsen over formålet ligger i den konkrete behandlingen. Bacon mfl. (2018) uttaler at hvor en node analyserer personopplysninger på sin lokale kopi av blokkjeden for å skaffe kommersiell innsikt, ansees noden som behandlingsansvarlig for personopplysningene.[172]

Forutsatt at nodene ansees som behandlingsansvarlige oppstår det spørsmål om nodene kan ansees som felles behandlingsansvarlige. Dette vil det redegjøres for i punkt 6.3.1.

6.2.4 Rollen til gruvearbeidere

Gruvearbeideren velger å kjøre en spesiell form for fullverdig node og har i teorien påvirkende innflytelse over hvorvidt en transaksjon samles i en blokk og sendes til nettverket for verifikasjon. I tillegg kan de, i likhet med noder, påvirke utviklingen av protokollen ved å akseptere eller avslå programvareoppdateringer til blokkjeden. Dette tilsier at gruvearbeidere har faktisk innflytelse over behandlingen av personopplysninger på blokkjeden.

CNIL har imidlertid lagt til grunn at gruvearbeidere kun validerer transaksjoner som er opprettet av brukerne og er ikke involvert i selve formålet med transaksjonen, og kan dermed ikke ansees som behandlingsansvarlige.[173] I lys av denne uttalelsen og parallellen til noder ansees det

[170] Ibid.
[171] Ibid.
[172] Ibid. s. 70
[173] CNILs veileder om blokkjeder (2018) s. 2.

nærliggende å slå fast at gruvearbeideren ikke har faktisk innflytelse over hvorfor de offentlige nøklene og transaksjonsdataen behandles i det konkrete tilfellet.

Spørsmålet er dermed om gruvearbeidere kan ansees som databehandlere som behandler «på vegne» av behandlingsansvarlig, jf. artikkel 4 nr. 8. Det forutsettes igjen at brukeren er behandlingsansvarlig.

Skullerud mfl. (2018) presiserer at ordlyden «på vegne» innebærer at «databehandleren ikke gjennomfører den aktuelle behandlingen for sitt eget formål, men har en rent kommersiell interesse i å levere den aktuelle tjenesten».[174] Formålet bak gruvearbeiderens deltakelse i blokkjede-nettverket og behandling av de offentlige nøklene og transaksjonsdataen er å få lønning for arbeidet (proof-of-work), samt innkassere eventuelle transaksjonsgebyrer. Dette innebærer at gruvearbeideren har kun rent kommersielle interesser i å validere transaksjonene.

Videre bestemmer gruvearbeideren hvilken programvare han skal laste ned og hvilken maskinvare som skal anvendes for å løse puslespillet. Gruvearbeidere kan dermed sies å ha faktisk innflytelse over de tekniske og organisatoriske midlene som skal anvendes i behandlingen. Disse avgjørelsene kan bestemmes eksklusivt av databehandler, jf. punkt 5.2.2.

Samlet sett kan gruvearbeidere ansees som databehandlere som behandler personopplysninger «på vegne» av brukeren for rent kommersielle interesser, jf. artikkel 4 nr. 8.

Imidlertid må det på tilsvarende måte som for noder skilles mellom gruvearbeidere som kun passivt kjører programvaren og behandler offentlige nøkler og transaksjonsdata på vegne av brukeren, og de som tar en mer aktiv rolle i behandlingen av personopplysningene. I slike tilfeller vil gruvearbeidere kunne identifiseres som behandlingsansvarlige.

6.2.5 Rollen til tilbydere av veksling- og oppbevaringstjenester

En bruker som ikke har lastet ned lommebok-programvaren som nevnt i punkt 3.5.3 kan generere nøklene hos en *tilbyder av oppbevaring- og vekslingstjenester for virtuell valuta.*

[174] Skullerud mfl. (2018) s. 62.

Hvitvaskingsforskriften 2018 § 1-3 har definert *oppbevaringstjenester* som «oppbevaring av private kryptografiske nøkler på vegne av kundene, for å overføre, lagre eller handle virtuell valuta». Brukeren har dermed sin private nøkkel og offentlige nøkler lagret hos en tredjepart.

Oppbevaringstjenesten kan være integrert på siden til tilbyderen av en *vekslingstjeneste*. Denne tjenesten kan ansees som en nettbørs for virtuell valuta. Ifølge Finanstilsynet tilbyr vekslingstjenester «kunder å handle eller veksle en type virtuell valuta til en offisiell valuta, for eksempel norske kroner, eller omvendt».[175] Tilgangen til tredjepartstjenesten får brukeren ved å logge seg inn på nettsiden som nett-klient.[176]

Tredjepartstjenesten oppbevarer brukerens private nøkkel og autoriserer at transaksjoner sendes til nettverket. Tredjeparten tar i tillegg imot personopplysninger som navn og mail-adresse for å inngå avtale med brukeren og være i tråd med blant annet reglene om hvitvasking.

Tredjepartstjenesten må ansees som en fullverdig node som initierer transaksjoner som del av sin virksomhet og bestemmer dermed formålet med behandlingen av personopplysningene til brukeren av tredjepartstjenesten. Tilbyder av oppbevaring- og vekslingstjenester for virtuell valuta må ansees som behandlingsansvarlig for personopplysningene til brukeren.

6.3 Problematikk knyttet til avtaleforhold mellom aktørene

6.3.1 Felles behandlingsansvar

I punkt 6.2 fremgår det at noder *kan* identifiseres som behandlingsansvarlige i visse tilfeller. Det må dermed vurderes om det foreligger felles behandlingsansvar mellom nodene på blokkjeden i henhold til GDPR artikkel 26. Dette vurderes på generelt grunnlag ettersom nodenes aktive rolle nodene i behandlingen av personopplysninger må vurderes konkret.

For det første må det vurderes hvorvidt noder behandler personopplysningene på blokkjeden «i fellesskap» i henhold til artikkel 26 nr. 1 første setning, jf. punkt 5.2.3.

Noder har som formål å oppnå stabilitet i nettverket. Nodene er likestilte og konsensus til den nåværende tilstanden til hovedboken nås når flertallet av nodene har validert transaksjonen.

[175] Finanstilsynet (2019).
[176] Antonopoulos (2015) s. 6. Eksempler på tilbydere av oppbevarings- og vekslingstjenester er www.kraken.no og www.coinbase.no.

Nodene har dermed påvirkende innflytelse over personopplysningene som behandles for sine egne formål, jf. Jehovas-Witness[177] Dette taler at for at nodene behandler personopplysningene «i fellesskap» for å oppnå stabilitet i nettverket.

Imidlertid har EU-domstolens avgjørelse om felles behandlingsansvarlig begrenset overføringsverdi til nodene ettersom de er selvstendige enheter som ikke har påvirkende innflytelse over de andre nodenes formål med behandlingen. En slik forståelse støttes av Michele Finck som uttaler at blokkjede nettverket er «[…] shaped by the nodes individual behaviour.»[178] Dette innebærer at nodene opprettholder driften av nettverket i felleskap, men avgjør individuelt *hvorfor* personopplysningene behandles.

Det ansees dermed uklart om nodene på blokkjeden behandler personopplysninger «i fellesskap» og må trolig avgjøres konkret for hver validering av en blokk. Kommer man frem til at nodene ikke behandler personopplysningene «i fellesskap» er nodene individuelle behandlingsansvarlige som trenger et selvstendig behandlingsgrunnlag for å overføre gruvearbeiderens blokk til neste node på nettverket. Eksempler på aktuelle behandlingsgrunnlag er inntatt i punkt 2.3, men vil ikke være gjenstand for nærmere vurdering i denne avhandlingen.

Forutsettes det at nodene bestemmer formålet med behandlingen «i fellesskap» må det vurderes hvorvidt aktørene har mulighet til å formalisere samarbeidet gjennom en «ordning» i henhold til artikkel 26 nr. 1 annen setning.

Formålet bak plassering av ansvar i tilfeller hvor flere aktører behandler personopplysninger er viktig for å kunne identifisere hvem de registrerte og datatilsynsmyndighetene kan rette seg mot, jf. fortalepunkt 79. Identifiseringen vil hindre ansvarspulverisering og sikre effektivt vern for de registrerte.

Formaliseringen av ansvar må sees i lys av de behandlingsansvarliges eksterne solidaransvar i artikkel 26 nr. 3. Det fremgår av bestemmelsen at «den registrerte kan utøve sine rettigheter i henhold til [GDPR] med hensyn til og overfor hver av de behandlingsansvarlige». Den

[177] C-25/17.
[178] Finck (2019) s. 100.

registrerte kan dermed utøve sine rettigheter overfor den behandlingsansvarlige de ønsker, «uavhengig av den interne ansvarsfordelingen mellom partene».[179]

Skullerud mfl. (2018) presiserer at solidaransvaret er «særlig viktig hvor en eller flere av de ansvarlige er mindre tilgjengelige, for eksempel som følge av geografisk plassering, eller mangler økonomisk evne til å bære et eventuelt erstatningskrav».[180] Slike tilfeller vil være særlig aktuelt for noder spredt over landegrenser og hvor den økonomiske evnen til noder varierer.

Imidlertid vil en ordning mellom nodene være vanskelig å gjennomføre i praksis. Tilgang til nettverket er åpent for alle og nodene representeres ikke med sin reelle identitet. Det stilles heller ingen regler eller betingelser for å melde seg inn i nettverket. I tillegg er ikke nodene forpliktet til å bli værende i nettverket og kan melde seg ut når de selv ønsker. Det ansees dermed ikke realistisk eller bærekraftig at flere hundre eller tusen noder med ukjente identiteter skal inngå en ordning som fordeler ansvar og forpliktelser i henhold til GDPR artikkel 26.

6.3.2 Forholdet mellom behandlingsansvarlig og databehandler

Forutsettes det at nodene (inkludert gruvearbeiderne) er databehandlere som behandler personopplysninger «på vegne» av brukeren stiller GDPR krav til at forholdet mellom partene reguleres. Forholdet mellom brukeren som behandlingsansvarlig og noder som databehandlere skal reguleres i en databehandleravtale, jf. GDPR artikkel 28 nr. 3. Avtalen skal regulere aktørenes rettigheter og forpliktelser for å sikre at behandling av personopplysninger skjer i henhold til GDPR.

Kravet til en databehandleravtale må sees i lys av at GDPR ble utformet for å regulere tjenester mellom sentraliserte aktører og tredjeparter. Imidlertid er ikke en slik formalisering overførbart til et desentralisert distribuert nettverk med ukjente aktører. I nettverket finnes det ikke en sentral juridisk enhet som representerer alle databehandlerne (nodene) i nettverket. Det er uklart hvordan en bruker av blokkjeden kan gi instruksjoner til nodene vedrørende behandling av offentlige nøkler og transaksjonsdata, når nodene er mange og ukjente.

[179] Skullerud mfl. (2018), s. 180.
[180] Ibid.

Det vil heller ikke være bærekraftig at brukeren skal måtte inngå en avtale med flere hundre eller tusen noder som kan delta eller frafalle fra nettverket når de selv ønsker og som ikke forholder seg til regler og betingelser ved innmeldingen.

Europarlamentets studie fra 2019, med henvisning til Bacon mfl. (2018), foreslår at programvareutviklerne kan sette betingelser til noder og brukere når de laster ned programvaren eller godtar programvareoppdateringer, og tilbydere av oppbevaring- og vekslingstjenester kan utarbeide betingelser for brukere som deltar i blokkjeden gjennom tredjeparten.[181] Det argumenteres at ved å designe plattformen i henhold til personvernlovgivningen vil dette kunne tiltrekke seg flere brukere, noder og gruvearbeidere til nettverket.[182]

En slik ordning vil imidlertid stride med hele konseptet til blokkjeden; den er betingelsesløs og protokollen angir de eneste reglene i blokkjeden. Blokkjeden skal ikke kunne styres fra et sentralisert kontrollpunkt og programvareutviklere skal ha en så liten rolle som mulig. En databehandleravtale i henhold til GDPR artikkel 28 nr. 3 som regulerer forholdet mellom brukeren og noder ansees dermed lite sannsynlig i lys av blokkjedens grunnleggende premisser.

[181] STOA (2019) s. 58, jf. Bacon mfl. (2018) s. 74-75.
[182] Ibid.

7 Konklusjon og avsluttende betraktninger

Funn i denne avhandlingen viser at offentlige nøkler til aktørene på blokkjeden og transaksjonsdata som inneholder personopplysninger som har blitt kryptert eller hashet til blokkjeden kvalifiseres som regel som «personopplysninger» i henhold til artikkel 4 nr. 1.

Konsekvensen er at man har en omfattende database med personopplysninger som ligger offentlig tilgjengelig på ubestemt tid. Dette reiser spørsmål om hvem som er ansvarlig for personopplysningene som registreres på blokkjeden.

Identifisering av behandlingsansvarlig på blokkjeden beror på hvem som har den faktiske innflytelsen over formålet med behandlingen og midlene som skal benyttes, jf. GDPR artikkel 4 nr. 7. Denne vurderingen ble analysert ut fra et mikronivå perspektiv ettersom personvernlovgivningen retter seg mot individuelle behandlinger av personopplysninger. I lys av denne vurderingen var det ulike aktører som kunne identifiseres som behandlingsansvarlige og databehandlere.

Grunnleggeren av blokkjeden og programvareutviklere stiller kun tilgjengelig et verktøy som andre kan benytte til sine egne formål og bestemmer ikke hvorfor eller hvordan verktøyet skal benyttes. De kan derfor ikke ansees som behandlingsansvarlige eller databehandlere.

Noder kan identifiseres som behandlingsansvarlige både der de oppfører seg som brukere og der de behandler personopplysningene for egne kommersielle formål. Ansees noder som behandlingsansvarlige kan det argumenteres for at de er felles behandlingsansvarlige. Det forutsettes imidlertid at de har en ordning seg imellom hvilket er uoppnåelig i praktiske termer.

I tillegg kan noder og gruvearbeidere være databehandlere for brukeren av blokkjeden ved å stille tilgjengelig databehandlingsressurser og behandle personopplysninger på vegne av brukeren. Gruvearbeidere vil som oftest ansees som databehandlere da de har økonomiske interesser i behandlingen av offentlige nøkler og transaksjonsdataen.

Uavhengig av om behandlingsansvar plasseres hos aktørene på blokkjeden vil de vanskelig kunne overholde mange av forpliktelsene som følger av GDPR. For eksempel vil ikke den registrerte kunne håndheve et krav om retting eller sletting av personopplysningene sine etter henholdsvis artikkel 16 og 17 ettersom dette ikke er mulig på blokkjeden. Nodene vil dermed være desentraliserte aktører som ikke har mulighet til å overholde sine forpliktelser.

Videre vil en klar allokering av ansvar mellom felles behandlingsansvarlige, og mellom behandlingsansvarlig og databehandlere, være lite praktisk i lys av blokkjedens egenskaper. Det vil i tillegg være problematisk for den registrerte å henvende seg til en individuell node ettersom identiteten til noden ikke er kjent. Dette kan føre til at den registrerte gir opp forsøket med å håndheve sine rettigheter under GDPR mot en eventuell behandlingsansvarlig, og vil som en konsekvens svekke personvernet til den registrerte.

Samlet sett viser forholdet mellom blokkjeder og GDPR hvordan regulatoriske rammeverk ligger bak teknologisk innovasjon. Blokkjeder bryter med den fundamentale oppbyggingen og forutsetningen i GDPR som retter seg mot aktører som har muligheten til å kontrollere tilgangsrettighetene i et system.

Blokkjeder er fortsatt en ung teknologi og det utvikles stadig flere kryptografiske teknikker som kan gjøre personopplysningene i en blokkjede anonyme. Det er likevel viktig med avklaring fra EU-domstolen og retningslinjer fra Personvernrådet for å fremme innovasjon av en teknologi som kan ha omfattende og positive konsekvenser for hvordan databaser drives i dag.

Ettersom blokkjeder ikke «passer» inn i forutsetningene til GDPR kan det være nødvendig med nye bestemmelser under GDPR eller nye reguleringer tilpasset blokkjeder som retter seg mot ansvar på åpne desentraliserte distribuerte databaser. Det bør utformes lovgivning som bryter med forutsetningen om et sentralisert kontrollpunkt og som fordeler ansvar over et nettverk.

Litteraturliste

7.1 Lover og forskrifter

Personopplysningsloven 2018	Lov om behandling av personopplysninger 15. juni 2018 nr. 31 (personopplysningsloven)
Hvitvaskingsforskriften 2018	Forskrift om tiltak mot hvitvasking og terrorfinansiering (hvitvaskingsforskriften) 14. september 2018 nr. 1324

7.2 EUs sekundærlovgivning

Personvernforordningen	EUROPAPARLAMENTETS- OG RÅDSFORORDNING (EU) 2016/579 av 27.4.2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger samt om oppheving av direktiv 95/46/EF [GDPR] OJ L 119, 4.5.2016, s. 1-88
Personverndirektivet	EUROPAPARLAMENTETS- OG RÅDSDIREKTIV 95/46/EF av 24.10.1995 om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger OJ L 281, 23.11.1995, s. 31-50

7.3 Rettspraksis fra EU-domstolen

Sak C-345/13	Dom av 19.06.2014, *Karen Millen Fashions* [ECLI:EU:C:2014:2013]
Sak C-434/16	Dom av 20.12.2017, *Peter Nowak* [ECLI:EU:C: 2017:994]
Sak C-210/16	Dom av 5. juni 2018, *Wirtschaftsakademie Schleswig v. Holstein* [EU:C:2017:796]
Sak C-25/17	Dom av 10.07.2018, *Jehovas Witness* [EU:C: 2018:551]
Sak C-40/17	Dom av 29.07.2019, *Fashion ID* [ECLI:EU:C: 2019:629]

Sak C-70/10	Dom av 24.11.2011, *Scarlet Extended* [ECLI:EU:C:2011:771]
Sak C-131/12	Dom av 13.05.2014, *Google Spain* [ECLI:EU:C:2014:317]
Sak C-212/13	Dom av 11.12.2014, *Ryneš* [EU:C:2014:2428]
Sak C-345/17	Dom av 14.02.2019,*Sergejs Buivids* [EU:C:2019:122]
Sak C-101/01	Dom av 6.11.2003, *Bodil Linqvist*[EU:C:2003:596]
Sak C-73/07	Dom av 16.12.2008, *Satamedia* [EU:C:2008:727]

7.4 Veiledere og uttalelser

A29WP Opinion 2/2007	Article 29 Data Protection Working Party, "*Opinion 2/2007 on the concept of personal data"*, 01248/07/EN WP 136 [Tilgjengelig på: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp140_en.pdf] (lest 22.09.2019)
A29WP Opinion 1/2010	Artikkel 29 Data Protection Working Party, "*Opinion 1/2010 on the concepts of "controller" and "processor"* 00264/10/EN WP 169 [Tilgjengelig på: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf] (lest 25.09.2019)
A29WP Opinion 05/2014	Article 29 Data Protection Working Party, "*Opinion 05/2014 on Anonymisation Techniques*, 0829/14/EN WP 216 [Tilgjengelig på: https://www.pdpjournals.com/docs/88197.pdf] (lest 17.10.2019)

7.5 Juridisk litteratur

7.5.1 Bøker

Fredriksen & Mathisen (2014) — Fredriksen, Halvard Haukland & Gjermund Mathisen. *EØS-rett*, 2. utgave, Fagbokforlaget, Bergen, 2014.

Finck (2019) — Finck, Michèle. *Blockchain regulation and governance in Europe.* Cambridge University Press, England, 2019.

Skullerud mfl. (2018) — Skullerud, Åste Marie Bergseng, Cecilie Rønnevik, Jørgen Skorstad & Marius Eng Pellerud. *Personvernforordningen (GDPR) Kommentarutgave*, Universitetsforlaget, Oslo, 2018. (lastet ned fra www.juridika.no 02.10.2019)

Wessel-Aas & Ødegaard (2018) — Wessel-Aas, Jon & Magnus Ødegaard. *Personvern – Publisering og behandling av personopplysninger*, 1. utgave, Gyldendal, Oslo, 2018. (lastet ned fra www.rettsdata.no 04.10.2019)

7.5.2 Artikler

Buocz mfl. (2019) — Buocz, Thomas, Tina Ehrke-Rabel, Elisabeth Hödl & Iris Eisenberger. *Bitcoin and the GDPR: Allocating responsibility in distributed networks.* (2019) Computer Law & Security Review, Volume 35 (2) [Tilgjengelig på: https://doi.org/10.1016/j.clsr.2018.12.003] (lest 20.10.19)

Bacon mfl. (2018) — Bacon, Jean, Johan David Michels, Christopher Millard & Jatinder Singh. *Blockchain Demystified: A Technical and Legal Introduction to Distributed and Centralised Ledgers.* (2018) Richmond Journal of Law and Technology, 25 (1) (lest 07.11.19)

Finck (2017) — Finck, Michèle. *Blockchains and Data Protection in the European Union*. (2017). Max Planck Institute for Innovation & Competition Research Paper No. 18-01 [Tilgjengelig på: http://dx.doi.org/10.2139/ssrn.3080322] (lest 09.09.2019)

7.5.3 Oppslagsverk

Olsen (2018) — Olsen, Thomas. *Kommentar til personopplysningsloven: Note (a4-8)* (28.09.2018) Norsk Lovkommentar [Tilgjengelig på: www.rettsdata.no] (hentet 09.12.2019)

7.6 Veiledere, studier og rapporter

CNILs veileder om blokkjeder (2018) — Commission Nationale de l'Informatique et des Libertés (CNIL). *Solutions for a responsible use of the blockchain in the context of personal data.* (06.11.2018) [Tilgjengelig på: https://www.cnil.fr/sites/default/files/atoms/files/blockchain.pdf] (lest 15.10.2019)

EBOF (2018) — Lyons, Tom, Ludovic Courcelas, Ken Timsit. Rapport av EBOF for EU-kommisjonen. *Blockchain and the GDPR.* (2018) [Tilgjengelig på: https://www.eublockchainforum.eu/reports] (lest 15.11.19)

EBOF (2019) — Lyons, Tom, Ludovic Courcelas, Ken Timsit. Rapport av EBOF for EU-kommisjonen. *Legal and regulatory framework of blockchains and smart contracts.* (2019) [Tilgjengelig på: https://www.eublockchainforum.eu/reports] (lest 15.11.2019)

Oppsummering av CNILs veileder om blokkjeder (2018) — Oppsummering av veilederen utformet av CNIL. *Solutions for a responsible use of the blockchain in the context of personal data*. (06.11.2016) [Tilgjengelig på: https://www.cnil.fr/en/blockchain-and-gdpr-solutions-responsible-use-blockchain-context-personal-data] (lest 21.10.2019)

STOA (2019) — Finck, Michèle. Studie av "the Panel for the Future of Science and Technology" (STOA). *Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European protection law?* (2019) Europarlamentet (EPRS) PE 634.445 [Tilgjengelig på: https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf] (lest 15.09.19)

7.7 Øvrige kilder

7.7.1 Bøker

Antonopoulos (2015) — Antonopoulos, Andreas M. *Mastering Bitcoin: Unlocking Digital Cryptocurrencies.* O'Reilly, 2015.

Drescher (2017) — Drescher, Daniel. *Blockchain Basics: A Non-Technical Introduction in 25 Steps.* Apress, 2017.

7.7.2 Nettsider

Bratbergsengen (2019) — Bratbergsengen, Kjell. *Database.* Store Norske Leksikon. (sist endret 12.11.2019) [Tilgjengelig på: https://snl.no/distribuert_database] (lest 28.09.2019)

Europakommisjonen (2018) — Europakommisjonen. Digital Market News. *European countries join Blockchain Partnership.* (10.04.18) [Tilgjengelig på: https://ec.europa.eu/digital-single-market/en/news/european-countries-join-blockchain-partnership] (lest 21.10.19)

Europakommisjonen (2019) — Europakommisjonen. Policy. *Blockchain technologies.* (Sist oppdatert 30.07.19) [Tilgjengelig på: https://ec.europa.eu/digital-single-market/en/blockchain-technologies] (lest 10.09.19)

Finanstilsynet (2019) — Finanstilsynet. *Virtuelle valutatjenester.* (31.01.19) [Tilgjengelig på: https://www.finanstilsynet.no/konsesjon/virtuelle-valutatjenester/] (lest 22.11.19)

Nakamoto (2008) — Nakamoto, Satoshi. *Bitcoin: A Peer-to-Peer Electronic Cash System* (2008) [Tilgjengelig på: https://bitcoin.org/bitcoin.pdf] (lest 09.10.2019)

Ray (2018) — Ray, Shaan. *The Difference Between Blockchains & Distributed Ledger Technology*. Towards Data Science. (20.02.2018) [Tilgjengelig på: https://towardsdatascience.com/the-difference-between-blockchains-distributed-ledger-technology-42715a0fa92] (lest 12.10.2019)

Rode (2017) — Rode, William. *Blockchain for non-techies: 1. Agreement* (01.06.2017) [Tilgjengelig på: https://medium.com/hackernoon/blockchain-for-non-techies-1-agreement-4a54857b82ba] (lest 14.11.2019)

Skramstad (2015) — Skramstad, Torbjørn. *Distribuert database.* Store Norske Leksikon (19.08.15) [Tilgjengelig på: https://snl.no/distribuert_database] (lest 28.09.19)

Lister over figurer

Figur 1:

Lastovetska (2019)	Lastovetska, Anastasiaa. *Architecture Basics: Components, Structure, Benefits and Creation.* (31.01.2019), [Tilgjengelig på: https://mlsdev.com/blog/156-how-to-build-your-own-blockchain-architecture] (hentet 23.09.2019)

Figur 3:

Skjermutklipp fra Ethereum-blokkjeden	Skjermutklipp fra Ethereum-blokkjedens individuelle transaksjoner i en konkret blokk. [Tilgjengelig på: https://www.blockchain.com/eth/block/9060074] (hentet 06.12.2019)

Figur 4:

Ray (2017)	Ray, Shaan. *Merkle Trees.* (14.12.2017) [Tilgjengelig på: https://hackernoon.com/merkle-trees-181cb4bc30b4] (hentet 15.11.19)

Figur 5:

Bacon mfl. (2018)	Bacon, Jean, Johan David Michels, Christopher Millard & Jatinder Singh. *Blockchain Demystified: A Technical and Legal Introduction to Distributed and Centralised Ledgers.* (2018) Richmond Journal of Law and Technology, 25 (1) (hentet 01.11.2019)

Figur 6:

Skjermutklipp fra Ethereum-blokkjeden	Skjermutklipp fra Ethereum-blokkjedens oversikt over nyeste blokker. [Tilgjengelig på: https://www.blockchain.com/explorer?view=eth_blocks] (hentet 06.12.2019)