Kryptovalutaen Bitcoin i lys av personvernforordningen

Er Bitcoin regulert av personvernforordningen og opererer kryptovalutaen i så fall i strid med forordningen som følge av dens manglende evne til å oppfylle brukernes rett til å bli glemt etter artikkel 17?

Kandidatnummer: 90

Antall ord: 12776

JUS399 Masteroppgave
Det juridiske fakultet

UNIVERSITETET I BERGEN

12 desember 2022

Innholdsfortegnelse

1. Innledning

1.1 Presentasjon av problemstillingen

I løpet av de ti siste årene har kryptovaluta gått fra å være en obskur trend blant IT-entusiaster til å bli et tema regelmessig behandlet i Norges største massemedier som et økonomisk fenomen man må ta på alvor.[1] Bitcoin, som er den første, største og meste kjente kryptovalutaen, passerte i 2013 en verdi på 1000 dollar for første gang.[2] I dag har kryptovalutaen en verdi på rundt 17 000 dollar, en nedgang fra den høyeste noteringen på hele 68 000 dollar fra den 10. november 2021.

Til tross for kryptovalutaers enorme markedsverdi på over 800 milliarder USD, blir dem sjeldent brukt til kjøp og salg av varer og tjenester i dagliglivet. I stedet blir kjøp av kryptovaluta i stor grad sett på som en investering med mulighet for stor avkastning som følge av dens volatile pris. Kryptovalutaer som Bitcoin er imidlertid utformet på en måte som gjør dem godt egnet til å bli bruk som dagligdags valuta. Man kan dermed ikke se bort ifra at kryptovalutaer kan bli en større del av hverdagen vår i fremtiden. Kanskje vil «kort eller krypto?» bli et vanlig spørsmål å høre når man skal betale på butikken?

Fremmarsjen av Bitcoin og andre kryptovalutaer har skjedd samtidig som bruken av internettbaserte tjenester har økt.[3] Utbredelsen av smarttelefoner har gitt oss et verktøy som gjør det mulig å være tilknyttet internettet til enhver tid. Internett har følgelig blitt en stor del av livene våre, noe som kan ha økt vår tillit til internettbaserte tjenester som Bitcoin. Denne utviklingen har imidlertid også gitt utviklerne av produktene en større mulighet til å tilegne seg store mengder data om brukeren.

Den økte bruken av internett har dermed gitt opphav til et større behov for personvern enn tidligere. Dette behovet ledet Den europeiske union (heretter EU) til å innføre «General Data Protection Regulation» (heretter GDPR, personvernforordningen eller forordningen) i 2018.[4] Forordningen legger føringer for hva som er tillatt bruk av personopplysninger, og ved brudd sanksjoneres det med betydelige overtredelsesgebyr.

[1] Se for eksempel https://www.nrk.no/sok/?q=Bitcoin
[2] Alle Bitcoin verdinoteringer hentes fra nettsiden Coinmarketcap, https://coinmarketcap.com/currencies/bitcoin/
[3] Se for eksempel https://www.ssb.no/teknologi-og-innovasjon/faktaside/internett-og-mobil
[4] Europaparlaments- og rådsforordning (EU) 2016/679 av 27. april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger

Det er klart at tradisjonelle nettbanker har gjort tilpasninger som følge av GDPR, men forordningen har tilsynelatende ikke påvirket utbredelsen av kryptovalutaer.[5] EU har ikke ilagt restriksjoner på bruken av kryptovalutaer og det var i 2021, tre år etter innføringen av GDPR, at Bitcoin hadde sin høyeste verdinotering. Videre er det klart at Bitcoin heller ikke har endret sin protokoll for å tilpasse seg kravene oppstilt etter GDPR, da det er svært vanskelig å endre den opprinnelige programvarekoden.[6]

Dette er interessant da Bitcoin opererer på blokkjedeteknologi som gjør det nærmest umulig å slette informasjon etter at det først har blitt lagret. Dette betyr at når informasjon først er lagret på Bitcoin-nettverket, vil informasjonen forbli på blokkjeden gjennom hele Bitcoin sin eksistens. Det er dermed vanskelig å se hvordan retten til å bli glemt etter GDPR artikkel 17 skal kunne praktiseres på Bitcoin-nettverket.

Dette reiser to interessante spørsmål som denne oppgaven skal forsøke å besvare; det første spørsmålet er om kryptovalutaer som Bitcoin blir regulert av GDPR. Det andre spørsmålet er, forutsatt at GDPR kommer til anvendelse på Bitcoin, vil Bitcoin operere i strid med forordningen som følge av at det tilsynelatende ikke er mulig å slette informasjon fra Bitcoin-nettverket. Problemstillingen for oppgaven blir derfor følgende:

> «Er Bitcoin regulert av personvernforordningen og opererer kryptovalutaen i så fall i strid med forordningen som følge av dens manglende evne til å oppfylle brukernes rett til å bli glemt etter artikkel 17?»

1.2 Avgrensning

I denne oppgaven vil problemstillingen besvares ut ifra et norsk perspektiv. Det vil dermed tas utgangspunkt i den norske rettstilstanden.

Videre vil det i denne oppgaven forutsettes at Bitcoin-brukerne har tilegnet seg Bitcoin på den mest personvernsvennlige måten som mulig. Dette innebærer tilegnelse ved kjøp gjennom en Bitcoin minibank med kontanter eller å motta Bitcoin som premie for gruvearbeid, som er det å stille maskinvare til rådighet for nettverket. Dette er en forutsetning som ikke nødvendigvis gjenspeiler virkeligheten, da det er svært vanlig å foreta kjøp på kryptobørser som Binance, Coinbase og Kraken. Disse nettsidene gjør det praktisk kjøpe Bitcoin, men enkelheten går på bekostning av anonymiteten. Kjøp gjennom disse nettsidene fordrer at man har en konto på

[5] Se for eksempel https://www.nordea.no/privat/kundeservice/general-data-protection-regulation.html og https://www.dnb.no/om-oss/personvern.html?la=NO&site=DNB_NO.
[6] Se kapittel 4.3 for konsensussystemet for endring på Bitcoin-nettverket

den gitte nettsiden og for å opprette en konto må man opplyse om navn, epostadresse, betalingsinformasjon og en form for offisiell identifikasjon. Slik kjøp av Bitcoin vil i det følgende avgrenses mot da det reiser personvernspørsmål med henhold til den spesifikke nettsiden man bruker og ikke Bitcoin i seg selv. I stedet vil oppgaven ta for seg bruk av Bitcoin som er i størst mulig grad anonym slik at man kan belyse personvernskonfliktene som teknologien i seg selv oppstiller.

2. Metode

2.1 Forholdet mellom norsk rett og GDPR

Behandling av personopplysninger blir i norsk rett regulert av personopplysningsloven og følgelig må analysen starte her.[7] Det fremgår av personopplysningsloven § 1 at personvernforordningen gjelder som lov, og av personopplysningsloven § 2 at «bestemmelsene i personvernsforordningen går i tilfelle konflikt foran bestemmelser i annen lov som regulerer samme forhold» jf. også EØS-loven § 2.[8] Man står da ovenfor to lovfestede rettskilder, hvor det ved motstrid vil være personvernsforordningen som får forrang. Den primære rettskilden må dermed være personvernsforordningen. En slik forståelse er også lagt til grunn i HR-2021-966-A hvor Høyesterett uttalte «Jeg finner det hensiktsmessig å forholde meg til forordningen også der personopplysningsloven har en parallell bestemmelse».[9] Dette medfører at personopplysningsloven kun er relevant i tilfeller hvor det kun er den som regulerer et forhold, ellers vil det være personvernsforordningen som er den primære rettskilden.

Videre følger det av EØS-avtalen artikkel 6 og ODA artikkel 3 nr. 1 at «Ved gjennomføringen og anvendelsen av bestemmelsene i [EØS-avtalen], og med forbehold for den fremtidige utvikling av rettspraksis, skal bestemmelsene, så langt de i sitt materielle innhold er identiske med de tilsvarende regler i [EU-retten], fortolkes i samsvar med de relevante rettsavgjørelser som [EU-domstolen] har truffet før undertegningen av [EØS-avtalen]».[10] Bestemmelsene gir uttrykk for at EØS-retten skal samsvare med EU-retten, også med hensyn til EU-domstolens

[7] Lov 15 juni 2018 nr. 38 om behandling av personopplysninger (personopplysningsloven)
[8] Lov 27 november 1992 nr. 109 om gjennomføring i norsk rett av hoveddelen i avtale om Det europeiske økonomiske samarbeidsområde (EØS-loven)
[9] HR-2021-966-A avsnitt 27
[10] Avtale av 2. mai 1992 mellom EFTA-statene om opprettelse av et overvåkningsorgan og en domstol, med protokollene 1 – 7 (ODA)

avgjørelser forut for avtaleinngåelsen. EØS-retten er følgelig bundet av EU-domstolens avgjørelser frem til bindingen.

Av ODA artikkel 3 nr. 2 følger det at ved fortolkningen og anvendelsen av EØS-retten skal det tas «tilbørlig hensyn til de prinsipper som er fastlagt gjennom de relevante rettsavgjørelser som [EU-domstolen] har truffet etter undertegningen av EØS-avtalen». Bestemmelsen gir uttrykk for at man i gjennomføringen av EØS-avtalen er sterkt bundet av prinsippene utledet av EU-domstolen også etter inngåelsen av EØS-avtalen.

Disse bestemmelsen sammenholdt gir uttrykk for en sentral del av homogenitetsprinsippet, hvor formålet er at reglene etter EØS-retten skal samsvare med reglene etter EU-retten.[11]

En slik forståelse av homogenitetsprinsippets rekkevidde er også lagt til grunn i HR-2022-328-A hvor Høyesterett slo fast at «Ved tolkning av forordningen veier EU-domstolens praksis tungt jf. EØS-avtalen artikkel 6».

Homogenitetsprinsippet medfører følgelig at ved tolkning av forordninger som er innlemmet i norsk rett gjennom EØS-avtalen, vil fortolkning i samsvar med relevante avgjørelser av EU-domstolen være nødvendig.

Da den primære rettskilden er personvernsforordningen, vil den metodiske innfallsvinkelen følge den EØS-rettslige metoden hvor formål og rettspraksis etter EU-domstolen er i fokus. Forordningens ordlyd vil dermed få en mindre fremtredende rolle enn hva som følger av norsk metodelære. Det vil i oppgaven likevel gjennomføres ordlydstolkninger for å raskt få et innblikk i hva bestemmelsen gir uttrykk for, men dersom denne tolkningen strider med rettspraksis eller forordningens formål, må tolkningen som følger av ordlyden vike. Dette skyldes at i EU-retten oversettes bestemmelsene til flere likestilte offisielle språk og det vil være umulig å ha den eksakt samme betydningen på tvers av språkene.[12]

Som følge av at ordlydstolkningen uansett har en mindre fremtredende rolle i utpenslingen av gjeldende rett, vil den uoffisielle norske oversettelsen av GDPR anvendes for å øke lesbarheten av oppgaven. Dersom det det skulle oppstå konflikt mellom den norske og de offisielle versjonene av GDPR med henhold til en bestemmelses ordlyd, vil denne konflikten presenteres og behandles.

[11] Finn Arnesen mfl., Oversikt over EØS-retten, Universitetsforlaget 2022, s. 41
[12] Johan Giertsen, Avtaler, 4, utgave, Universitetsforlaget 2021, s. 33

2.2 Særlige metodiske utfordringer

En metodisk utfordring i forsøket på å besvare oppgavens problemstilling er den gjennomgående mangelen på autorative rettskilder på området. Kryptovaluta har aldri blitt direkte behandlet av EU, verken i lovgivningen eller i domstolen. Dette medfører at oppgavens behandling av den overordnete problemstillingen bygger på kilder som ikke nødvendigvis har direkte overføringsverdi til kryptovalutaer.

Videre er en annen utfordring at GDPR som er den primære rettskilden på området er nytt. Dette medfører at forordningen fortsatt inneholder usikkerheter som ikke har blitt avklart i rettskildene. Siden oppgaven behandler forholdet mellom GDPR og en desentralisert kryptovaluta, noe som ikke kan anses å være i kjernen av GDPR, oppstår det flere slike usikkerheter i løpet av analysen. I mangel på rettskilder med henhold til GDPR som avklarer disse usikkerhetene, brukes rettskildene som knytter seg til den erstattede direktiv 95/46 isteden. I hvilken grad disse rettskildene har direkte overføringsverdi til GDPR er imidlertid usikkert.

Oppgavens analyse bygger dermed på rettskilder som ikke nødvendigvis har direkte overføringsverdi til Bitcoin regulert etter GDPR. Dette medfører et usikkerhetsmoment med henhold til oppgavens konklusjon.

3. Presentasjon av personvernforordningen

GDPR er en forordning iverksatt mai 2018 som omhandler personvern og datasikkerhet. Formålet med forordningen er å verne fysiske personer i forbindelse med behandling av personopplysninger jf. GDPR fortalepunkt 1. Forordningen har sitt utspring av retten til privatliv etter menneskerettskonvensjon artikkel 8 første ledd som har følgende ordlyd:

> «Enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin korrespondanse»[13]

Og av retten til vern av personopplysninger etter EUs pakt om grunnleggende rettigheter artikkel 8 som har følgende ordlyd:

> «Protection of personal data
>
> 1. Everyone has the right to the protection of personal data concerning him or her.

[13] Europarådets konvensjon 4. november 1950 om beskyttelse av menneskerettighetene og de grunnleggende friheter som endret ved femtende protokoll 24. juni 2013

> 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
>
> 3. Compliance with these rules shall be subject to control by an independent authority»[14]

Forordningen regulerer hvordan aktører kan behandle personopplysninger og ved brudd kan det ilegges overtredelsesgebyr. Gebyret for de mest alvorlige overtredelsene reguleres i GDPR artikkel 83 femte ledd som har følgende ordlyd:

> «Ved overtredelser av følgende bestemmelser skal det i samsvar med nr. 2 ilegges overtredelsesgebyr på opptil 20 000 000 euro eller, dersom det dreier seg om et foretak, på opptil 4% av den samlede globale årsomsetningen i forutgående regnskapsår, der det høyeste beløpet anvendes»

Brudd på GDPR straffes følgelig med betydelige bøter som er avhengig av bruddets alvorlighet og den ansvarliges økonomiske stilling. Videre skal det sikres at gebyrene er «virkningsfull, står i et rimelig forhold til overtredelsen og virker avskrekkende» etter GDPR artikkel 83 første ledd.

For å bedre forstå betydningen av GDPR vil tre eksempler på saker avgjort på grunnlag av GDPR kort presenteres.

I 2019 ble Google ilagt et overtredelsesgebyr på 50 millioner euro av det franske datatilsynet CNIL. Årsaken til gebyret var Googles manglende klarhet med henhold til retningslinjene knyttet til personalisert reklame. Informasjonen var vanskelig å finne og følgelig hadde ikke brukerne en reell rett til å avvise alternativet om personalisert reklame, noe man har en rett til etter GDPR.[15]

[14] Den europeiske unions charter om grunnleggende rettigheter av 1. desember 2009
[15] Alex Hern, «Google fined record £44 by french data protection watchdog», The Guardian, 21. januar 2019, https://www.theguardian.com/technology/2019/jan/21/google-fined-record-44m-by-french-data-protection-watchdog

I 2020 ble H&M bøtelagt med 35 millioner euro av datatilsynet i Tyskland. Bakgrunnen for gebyret var selskapets overvåkning av de ansette ved å lagre data om de ansattes familie, religion og sykdom, noe som er i strid med GDPR.[16]

Per dags dato er den største boten utstedt på bakgrunn av GDPR på hele 747 millioner euro. Boten ble ilagt Amazon av datatilsynet i Luxembourg. Det er imidlertid få detaljer om saken som har blitt offentliggjort, men saken skal ha omhandlet personopplysninger med henhold til personalisert reklame.[17]

4. Presentasjon av kryptovalutaen Bitcoin

Før man starter med den juridiske analysen av forholdet mellom Bitcoin og GDPR, er det viktig å ha en grunnleggende forståelse for hvordan kryptovalutaer fungerer. I inneværende kapittel vil Bitcoin og den underliggende teknologien kort presenteres, i den grad det er nødvendig for å forstå den øvrige analysen.

4.1 Innledning Bitcoin

I oktober 2008, ble en vitenskapelig artikkel publisert på Bitcoin.org under pseudonymet «Satoshi Nakamoto».[18] Artikkelen var kalt «Bitcoin: A Peer-to-Peer Electronic Cash System» og er vårt første møte med kryptovalutaen som i dag har en markedsverdi på over 300 milliarder dollar.[19] Satoshi viser i artikkelen misnøye med hvordan man ved handel på internett er totalt avhengig av tredjeparts finansielle institusjoner til å prosessere kjøp, og foreslår dermed et alternativ. Den hypotetiske løsningen, kalt Bitcoin, presenteres som en heldigital valuta som kan overføres mellom personer uten å måtte gå gjennom en finansiell institusjon.[20] Den 3. januar 2009, fire måneder etter publikasjonen av artikkelen, ble den første Bitcoin-blokken utvunnet og kryptovalutaeventyret var i gang.[21]

[16] Forfatter ikke opplyst, BBC, «H&M fined for breaking GDPR over employee surveillance», 5. oktober 2020, https://www.bbc.com/news/technology-54418936
[17] Carly Page, TechCrunch, «EU hits Amazon with record-breaking $887M GDPR fine over data misuse», 30. juli 2021, https://techcrunch.com/2021/07/30/eu-hits-amazon-with-record-breaking-887m-gdpr-fine-over-data-misuse/
[18] Satoshi Nakamoto, «Bitcoin: A Peer-to-Peer Electronic Cash System», oktober 2008, https://bitcoin.org/en/bitcoin-paper
[19] Markedsverdi hentet fra https://coinmarketcap.com/currencies/bitcoin/
[20] Nakamoto (2008) s. 1.
[21] Connor Murray, «The mystery of the Genesis block», Coingeek, 7. desember 2021, https://coingeek.com/the-mystery-of-the-genesis-block/

4.2 Kryptovaluta

En kryptovaluta er en desentralisert digital valuta som overføres mellom deltakere gjennom et node-til-node-nettverk, hvor en node er et begrep for hver enkelt deltaker som er tilkoblet nettverket.[22]

Kryptovalutaer skiller seg fra tradisjonelle valutaer ved at de er frigjort fra tredjepartsaktører. Kryptovalutaer har ingen sentralbank som styrer deres pengepolitikk slik som tradisjonelle valutaer som USD, NOK og EURO. Videre kan kryptovalutaer operere digitalt uten bruken av tredjeparter.[23] Overføring av kryptovalutaer skjer direkte mellom deltakerne, uten behov for å legge sin tillit i en nettbank.[24]

Dersom Peder ønsker å overføre 100 kroner digitalt til Lars, må dette skje ved hjelp av en tredjepart, slik som nettbanken til DnB. Overføringsprosessen skjer dermed ved at DnB reduserer verdien på Peder sin konto, og øker verdien tilsvarende hos Lars. DnB fungerer dermed som et nødvendig mellomledd for at transaksjonen kan finne sted. Hvis Peder ønsker å overføre 1 Bitcoin til Lars, er det ikke nødvendig med et slikt mellomledd, da transaksjonen kan skje direkte mellom Peder og Lars på Bitcoin-nettverket.

Ved bruk av kryptovaluta er man heller ikke avhengig av tredjeparter for å lagre verdier digitalt, slik man er ved tradisjonelle valutaer. Dersom man ønsker å lagre verdier i kroner, er man avhengig av f.eks. DnB sin nettbankløsning. Ved kryptovaluta kan man imidlertid selv lagre egen valuta på egen maskinvare, helt uavhengig av involvering av tredjeparter.

I eksempelet ovenfor tilbyr DnB plattformen som gjør det mulig å lagre og overføre NOK mellom individer, men dette fører også med seg et stort ansvar. Ved å bruke DnB sin plattform legger man tillit i at de vil klare å håndtere problemene som kan oppstå ved å drifte et slikt nettverk. Dette inkluderer f.eks. det å validere at en faktisk har nok penger til å gjennomføre en overførsel, forhindre dobbeltbetaling av en sum foretatt på samme tid til forskjellige mottakere, unngå at verdier går tapt som følge av datafeil og å forhindre uautoriserte overføringer. Videre er det også en fare for manipulasjon av kontoer, enten internt eller av eksterne hackere. Det er dermed mye som kan gå galt og tilliten til å unngå disse feilene er plassert på et fåtall aktører som tilbyr nettbanktjenester for tradisjonell valuta.

[22] Jake Frankenfield, «Cryptocurrency Explained With Pros and Cons for Investment», Investopedia, 26. september 2022, https://www.investopedia.com/terms/c/cryptocurrency.asp (lest 1. november 2022)
[23] Ibid
[24] Nakamoto (2008) s. 1

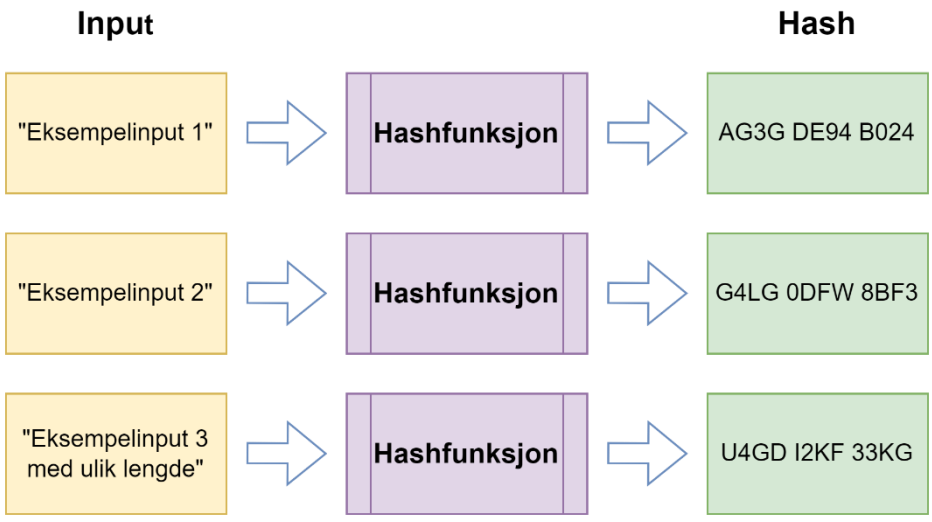
I stedet for å legge denne tilliten i tredjepartsbanker, unngår kryptovalutaer disse problemene ved hjelp av blokkjedeteknologi.

4.3 Blokkjeder

En blokkjede er en distribuert database som er lagret i nodene i et nettverk. Data blir lagret på blokker som henger sammen og som dermed danner blokkjeder. Disse blokkene blir deretter som helhet distribuert til hver av nodene i nettverket.[25]

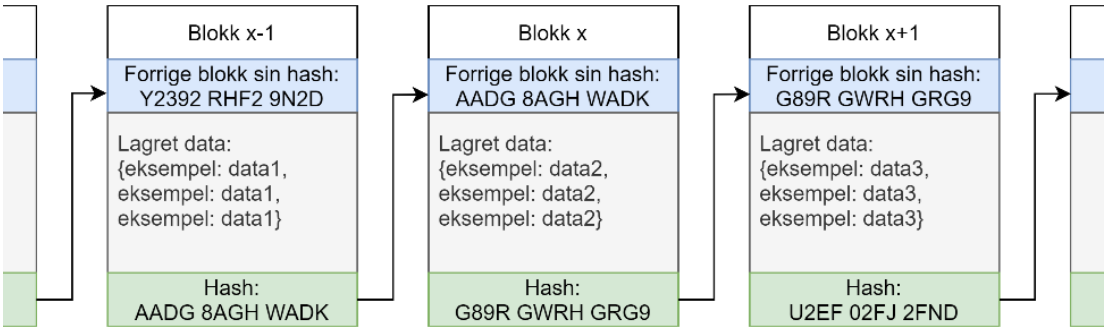
En blokk er en datastruktur som kan lagre informasjon og som kan henge sammen som en blokkjede. En blokkjede må inneholde tre viktige elementer: den lagrede informasjonen, en «hash» og den foregående blokken sin «hash» utviklet av en «hashfunksjon».[26]

En hasjfunksjon er en matematisk funksjon hvor man legger inn data av varierende lengde som input og får en kode av en fastsatt lengde, kalt en hash, som resultat. En hashfunksjon vil alltid gi det samme resultatet ved samme input, dermed vil en hash være basert på informasjonen den er produsert av.[27] Siden hver blokk inneholder den foregående blokken sin hash, inneholder de informasjon om den foregående blokkens innhold, dermed henger blokkene sammen i kjeder. Det er av den årsak teknologien kalles blokkjedeteknologi.[28]



Figur 1 - Eksempel av hashfunksjon

[25] Adam Hayes, «Blockchain Facts: What Is It, How It Works, and How It Can Be Used», Investopedia, 27. september 2022, https://www.investopedia.com/terms/b/blockchain.asp
[26] Ibid
[27] Forfatter ikke opplyst, «Cryptography Hash Functions», Tutorialspoint, uten år, https://www.tutorialspoint.com/cryptography/cryptography_hash_functions.htm
[28] Hayes (2022)



Figur 2 - Eksempel på et utdrag av en blokkjede

Når ny informasjon skal legges til i blokkjeden, kunngjøres informasjonen i nettverket slik at hver av nodene mottar denne informasjonen og lagrer informasjonen på egen blokk. Etter at informasjon har blitt lagret og validert, legges blokken til i blokkjeden til hver av nodene i nettverket. Etter at informasjon har blitt lagret i blokkjeden er det svært vanskelig å endre eller slette informasjonen. Dette er som følge av at blokkjeder av design er «immutable» noe som betyr at de ikke kan endres i ettertid. Det er kun mulig legge til ny informasjon.[29] Det er denne egenskapen med blokkjeder som gir opphav til problematikken som presenteres i problemstillingen med henhold til Bitcoin. Siden Bitcoin er basert på blokkjedeteknologi hvor det i utgangspunktet ikke er mulig å slette informasjon etter lagring, kan dette tilsi at Bitcoin opererer i strid med GDPR som følge av deres manglende evne til å ivareta retten til å bli glemt etter GDPR artikkel 17.

Ettersom hver node oppdaterer sin blokkjede basert på den samme informasjonen som de øvrige nodene i nettverket, er utgangspunktet at hver av blokkjedene er like. Det kan imidlertid oppstå programvarefeil eller eksterne hackerangrep, som kan føre til at ikke alle blokkjedene er identiske. For å løse denne problematikken opererer blokkjedeteknologi med et sikkerhetssystem basert på konsensus.[30] Dersom nettverket på et tidspunkt har flere enn én versjon av blokkjeden lagret, vil hver av nodene «stemme» på sin versjon av blokkjeden. Deretter vil den versjonen med høyest oppslutning av stemmene anses som den riktige versjonen, slik at den spres gjennom nettverket og lagres i alle nodene. På denne måten vil kryptovalutaer kjapt identifisere forsøk på manipulasjon og løse problemet.

Dersom man ønsker å endre eller slette informasjon fra en blokkjede til tross for blokkjeders uforanderlige karakter, må dette gjennomføres ved å oppnå konsensus i nettverket. For å gjøre

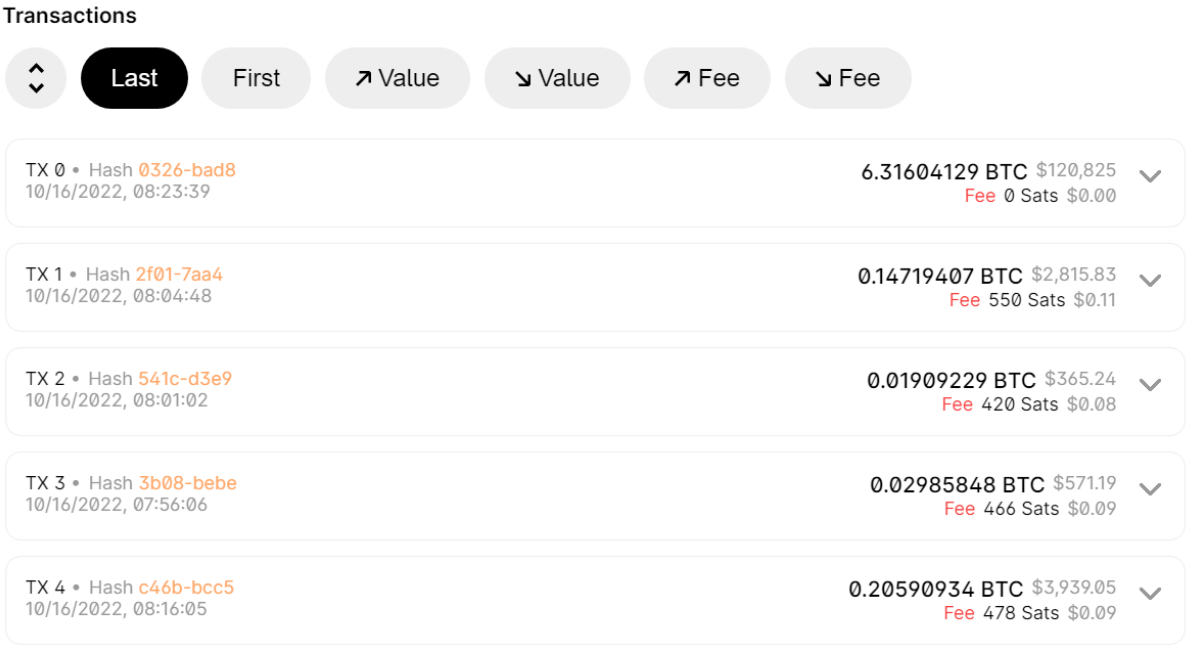
[29] Ibid
[30] Ibid

dette må man endre informasjonen i flertallet av nodene, slik at den nye versjonen oppnår konsensus i nettverket.

4.4 Hvilken informasjon lagres på Bitcoin sin blokkjede

Som det vil ses nærmere på i kapittel 5.3, kommer GDPR kun til anvendelse på behandling av personopplysninger. Det vil derfor i inneværende delkapittel kartlegges hvilken informasjon som lagres på Bitcoin-nettverket, for å få den nødvendige oversikten for en juridisk analyse senere. Denne analysen vil foretas i delkapittel 5.3.4.

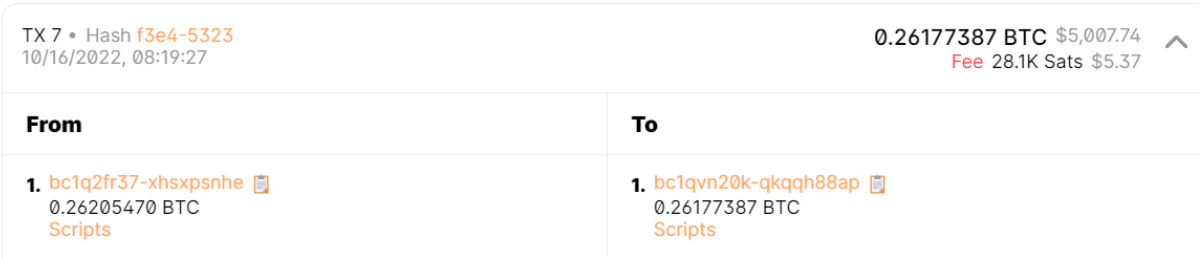
All informasjon som lagres på Bitcoin-nettverket er tilgjengelig for offentligheten og kan finnes på Blockchain.com. I eksempelet fremover vil blokk nummer 758 892 brukes som et eksempel for å kartlegge hvilke data som lagres.[31]



Figur 3- Eksempel på transaksjoner lagret på blokk

Som man kan se på figur 3 kan man inne på hver blokk se at det er lagret en lang rekke med Bitcoin-transaksjoner. Hver av disse transaksjonene kan man trykke seg inn på for å få flere detaljer.

[31] https://www.blockchain.com/explorer/blocks/btc/758892



Figur 4 - Eksempel på detaljer om en transaksjon lagret på blokk

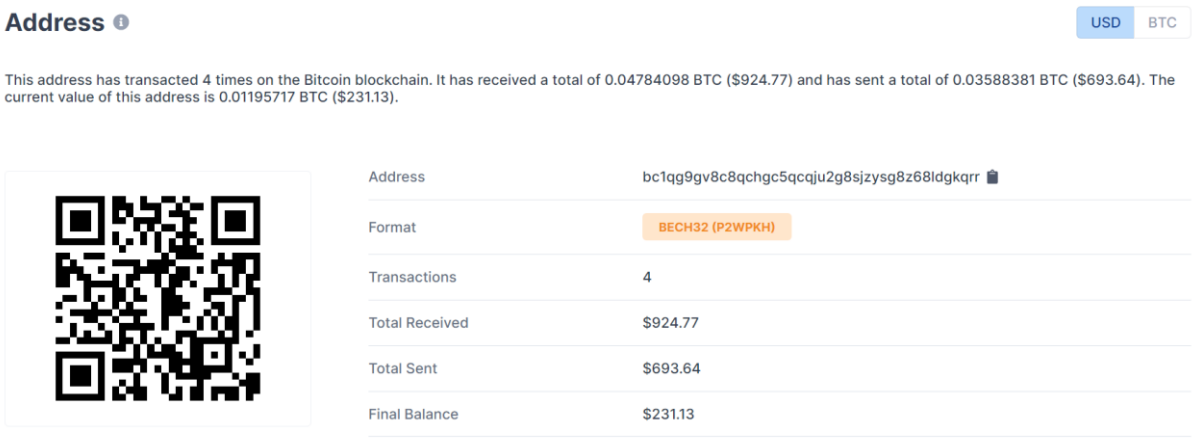
I transaksjonen i figur 4 kan man se at 0,26 Bitcoin ble overført den 16 november 2022 klokken 08:19:27 fra «bc1q2fr37-xhsxpsnhe» til «bc1qvn20k-qkqqh88ap». Videre kan man se at på transaksjonstidspunktet hadde 0,26 Bitcoin en verdi på drøyt fem tusen dollar.

Koden man ser i feltet for sender og mottaker gir uttrykk for senders og mottakers adresse til deres digitale lommebøker. Denne adressekoden blir også kalt lommebokens offentlige nøkkel og det er her verdiene på nettverket lagres. Hvem som helst på Bitcoin-nettverket kan sende verdier til en digital lommebok, men for å kunne råde over verdiene lagret i den digitale lommeboken, kreves det også en privat nøkkel. Denne private nøkkelen er en kode som det kun er den som opprettet lommeboken som har tilgang til.

Dersom man han hadde hatt kjennskap til hvem eierne av disse lommebøkene er, kunne transaksjonen blitt oversatt til følgende:

«Peder Ås sendte den 16 november 2022 klokken 08:19:27 5000 dollar til Lars Holm.»

Informasjonen som er lagret på hver av lommebøkene er også offentlige. Man kan dermed trykke seg inn på en gitt lommebok og se antall transaksjoner, hvor mange Bitcoin man har sendt og mottatt, hvor mye man har på konto, samt detaljer om hver transaksjon man har foretatt.



Figur 5 - eksempel på informasjon lagret på den digitale lommeboken

Dersom man hadde hatt kunnskap om hvem som var eier av lommeboken presentert i figur 5 hadde man hatt kjennskap til personens økonomiske balanse, samt hvem personen har sendt og mottatt penger fra. Informasjonen kunne dermed blitt oversatt til følgende:

«Den 10. november mottok Marthe 500 dollar fra Peder. Tre dager senere mottok hun ytterligere 424 dollar. Samme dag brukte hun 493 dollar i en klesbutikk. I tillegg overførte hun 200 dollar til en venninne. Marthe har nå 231 dollar igjen.»[32]

På Bitcoin-nettverket deles det dermed informasjon om både økonomisk balanse og transaksjonshistorikk. Hvem informasjonen knytter seg til er imidlertid skjult, da det kun er den offentlige nøkkelen til de aktuelle lommebøkene som deles. Hva som er identiteten til personene bak lommebøkene blir ikke delt.

5. Kommer GDPR til anvendelse på Bitcoin?

5.1 Presentasjon av GDPR sitt anvendelsesområde

Nå som både GDPR og teknologien bak kryptovalutaen Bitcoin har blitt presentert, vil resten av oppgaven ta for seg problemstillingen og forsøke å gi et svar basert på en nærmere analyse. Det minnes om at problemstillingen oppgaven forsøker å besvare er følgende:

> «Er Bitcoin regulert av personvernforordningen og opererer kryptovalutaen i så fall i strid med forordningen som følge av dens manglende evne til å oppfylle brukernes rett til å bli glemt etter artikkel 17?»

Det første steget i å besvare problemstillingen er å vurdere om GDPR kommer til anvendelse på Bitcoin. Spørsmålet blir dermed om vilkårene knyttet til det geografiske og materielle anvendelsesområde etter GDPR er oppfylt slik at forordningen kommer til anvendelse. Det er disse innledende vilkårene som skal behandles i inneværende kapittel.

5.2 GDPR sitt geografiske anvendelsesområde

GDPR sitt geografiske anvendelsesområde blir regulert i GDPR artikkel 3. Bestemmelsens første og annet ledd har følgende ordlyd:

> «1. Denne forordning får anvendelse på behandling av personopplysninger som utføres i forbindelse med aktivitetene ved virksomheten til en behandlingsansvarlig

[32] Et oppdiktet scenario basert på informasjonen om adresse «bc1qg9gv8c8qchgc5qcqju2g8sjzysg8z68ldgkqrr». Transaksjonene samsvarer ikke med transaksjonene som adressen har foretatt.

eller en databehandler i Unionen, uavhengig av om behandlingen finner sted i Unionen eller ikke.

2. Denne forordning får anvendelse på behandling av personopplysninger om registrerte som befinner seg i Unionen, og som utføres av en behandlingsansvarlig eller databehandler som ikke er etablert i Unionen, dersom behandlingen er knyttet til

a. tilbud av varer eller tjenester til slike registrerte i Unionen, uavhengig av om det kreves betaling fra den registrerte eller ikke, eller

b. monitorering av deres atferd, i den grad deres atferd finner sted i Unionen»

En naturlig språklig forståelse av bestemmelsens gir uttrykk for at forordningen har et vidt anvendelsesområde; dersom den registrerte eller den ansvarlige befinner seg i EU, vil GDPR komme til anvendelse.

En slik forståelse fremgår også av veileder 3/2018 som er en veileder til forordningens territorielle anvendelsesområde utgitt av EUs personvernsråd.[33] Her utledes det:

«Article 3 of the GDPR defines the territorial scope of the Regulation on the basis of two main criteria: the "establishment" criterion, as per Article 3(1), and the "targeting" criterion as per Article 3(2). Where one of these two criteria is met, the relevant provisions of the GDPR will apply to relevant processing of personal data by the controller or processor concerned».

Veilederen gir dermed uttrykk for at det er tale om to alternative vilkår, noe som samsvarer med tolkningen som fremgår av bestemmelsens ordlyd. Denne forståelsen legges følgelig til grunn.

Hvorvidt Bitcoin innfrir det geografiske anvendelsesområdet etter bestemmelsens første ledd, avgjøres basert på om virksomheten til en «behandlingsansvarlig» er lokalisert i EU. Dette introduserer et spørsmål om hvem som er behandlingsansvarlig på Bitcoin-nettverket.

Av GDPR artikkel 4 punkt 7 kan man lese følgende definisjon av en behandlingsansvarlig:

«behandlingsansvarlig» en fysisk eller juridisk person, en offentlig myndighet, en institusjon eller ethvert annet organ som alene eller sammen med andre bestemmer formålet med behandlingen av personopplysninger og hvilke midler som skal

[33] European Data Protection Board, «Guidelines 3/2018 on the territorial scope of the GDPR (Article 3)», 12. november 2019, s. 4.

> benyttes; når formålet med og midlene for behandlingen er fastsatt i unionsretten eller i medlemsstatenes nasjonale rett, kan den behandlingsansvarlige, eller de særlige kriteriene for utpeking av vedkommende, fastsettes i unionsretten eller i medlemsstatenes nasjonale rett»

Som det fremgår av utdraget er kjernen i bestemmelsen at «behandlingsansvarlig» er den som «bestemmer formålet med behandlingen av personalopplysninger og hvilke midler som skal benyttes». I Bitcoin sitt tilfelle er det tilsynelatende ingen som verken bestemmer formålet med behandlingen eller hvilke midler som skal benyttes, da Bitcoin kun er et nettverk med allerede fastsatte regler som det er svært vanskelig å endre i ettertid.[34] Dette kan tilsi at det ikke er noen behandlingsansvarlige på nettverket og at GDPR artikkel 3 første ledd dermed ikke er treffende. Siden det geografiske anvendelsesområdet uansett kan innfris basert på brukernes lokasjon etter bestemmelsens annet ledd, vil problematikken rundt hvem som er behandlingsansvarlig ikke drøftes videre i denne oppgaven. Det kan imidlertid nevnes at basert på analysene i «Can distributed ledgers be squared with European data protection law?» av Finck og masteroppgaven «Hvem er ansvarlig for personopplysninger i blokkjeder?» av Rode, kan det antydes at det er tale om et delt ansvar mellom alle nodene i nettverket.[35] Dersom det er tilfelle vil det uansett være vanskelig å konstatere en eksakt lokasjon for de behandlingsansvarlige og at GDPR artikkel 3 første ledd uansett ikke er treffende.

Som følge av at det geografiske anvendelsesområdet etter GDPR artikkel 3 første ledd ikke er treffende, må det ses nærmere på er om Bitcoin oppfyller bestemmelsens annet ledd slik at forordningen likevel kommer til anvendelse.

Ifølge veileder 3/2018 er vurdering av «targeting»-kriteriet etter annet ledd todelt. For det første må det avgjøres om det foregår behandling av personopplysninger av «registrerte som befinner seg i Unionen», for det andre må det vurderes om det er tale om «tilbud av varer og tjenester» til den registrerte lokalisert i Unionen etter bestemmelsens punkt a eller «monitorering av deres atferd» etter punkt b.[36]

[34] Se kapittel 4.3 for konsensussystemet for endring på Bitcoin-nettverket
[35] Dr Michèle Finck, European Parliamentary Research Service, «Blockchain and the General Data Protection Regulation – Can distributed ledgers be squared with European data protection law?», juli 2019, kapittel 4.3.3; Ane Victoria Rode, «Hvem er ansvarlig for personopplysninger i blokkjeder?», 10 desember 2019, s. 53
[36] Ibid s. 14

Siden Bitcoin-nettverket strekker seg verden over, er det klart at Bitcoin også har brukere i EU. Vilkåret om at det foreligger «registrerte som befinner seg i Unionen» er følgelig oppfylt.

Videre er det også uproblematisk å konstatere at Bitcoin må anses som «tilbud av (…) tjenester» da Bitcoin er et nettverk som gjør det mulig å overføre verdier digitalt. Punkt a er følgelig er oppfylt.

Dette medfører at Bitcoin innfrir GDPR sitt geografiske anvendelsesområde etter «targeting»-kriteriet som fremgår av GDPR artikkel 3 annet ledd punkt a.

5.3 GDPR sitt materielle anvendelsesområde

Nå som det er konstatert at Bitcoin innfrir vilkårene for å inngå i det territorielle anvendelsesområde til GDPR, er det neste steget å vurdere om også vilkårene for GDPR sitt materielle anvendelsesområde er oppfylt. Dersom det er tilfelle, betyr det at begge inngangsvilkårene for GDPR er innfridd og at forordningen kommer til anvendelse på Bitcoin.

Personvernsforordningens materielle virkeområde blir regulert i GDPR artikkel 3. Bestemmelsens første ledd har følgende ordlyd:

> «Denne forordning får anvendelse på helt eller delvis automatisert behandling av personopplysninger og på ikke-automatisert behandling av personopplysninger som inngår i eller skal inngå i et register»

Utdraget gir uttrykk for at forordningen får anvendelse på «helt eller delvis automatisert» «behandling» av «personopplysninger». Det er på det rene at det på Bitcoin-nettverket foregår «helt eller delvis automatisert» «behandling» av personopplysninger da det automatisk lagres og prosesseres data jf. GDPR artikkel 4 punkt 2.

Det problematiske vilkåret er følgelig om dataen på Bitcoin-nettverket må anses som «personopplysninger».

5.3.1 «Personopplysninger»

Som utpenslet i avsnitt 4.4 lagrer Bitcoin-nettverket informasjon om en lommeboks balanse og dens transaksjonshistorikk. Det må dermed vurderes om denne informasjonen er å anse som «personopplysninger», slik at vilkåret er oppfylt og at Bitcoin må anses å være innenfor GDPR sitt materielle anvendelsesområde.

Formålet med GDPR er nettopp det å verne enkeltindivider i forbindelse med behandlingen av deres personopplysninger, se f.eks. GDPR fortalepunkt nummer 1. Hva som er å anse som en personopplysning er dermed en svært sentral del av GDPR og som dermed må behandles i dybden.

En naturlig språklig forståelse av formuleringen «personopplysninger» tilsier at vilkåret er todelt; for det første må det være tale om en opplysning og for det andre må opplysningen være relatert til en person. Dette tilsier at vilkåret tar sikte på å omfatte enhver opplysning som omhandler en person.

Begrepet «personopplysninger» er videre utdypet i GDPR artikkel 4 som definerer sentrale begreper i forordningen. Bestemmelsens første ledd sammenholdt med bestemmelsens innledning gir følgende ordlyd:

> «I denne forordningen menes med
> 1. «personopplysninger» enhver opplysning om en identifisert eller identifiserbar fysisk person («den registrerte»); en identifiserbar fysisk person er en person som direkte eller indirekte kan identifiseres, særlig ved hjelp av en identifikator, f.eks. et navn, et identifikasjonsnummer, lokaliseringsopplysninger, en nettidentifikator eller ett eller flere elementer som er spesifikke for nevnte fysiske persons fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sosiale identitet»

Ut ifra bestemmelsens ordlyd kan man oppstille fire kumulative vilkår som må være til stede for at det skal være tale om en personopplysning. Disse er «enhver opplysning» «om» en «identifisert eller identifiserbar» «fysisk person».

Definisjonen av en personopplysning etter GDPR er identisk med den som følger av den erstattede direktiv 95/46 artikkel 2 bokstav a hvor det utledes at en personopplysning er «any information relating to an identified or identifiable natural person».[37] Som følge av at de to bestemmelsene er identiske, legges det til grunn at forståelsen av «personopplysninger» etter GDPR ikke er ment å være en realitetsendring sammenlignet med begrepet etter direktiv 95/46. Vilkårene må dermed antas å måtte tolkes likt. Ved mangel på autorative rettskilder som knytter seg til «personopplysninger» etter GDPR, vil rettskilder til den gamle bestemmelsen dermed være relevante tolkningsbidrag.

[37] Europaparlamentets og Rådets direktiv 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.

I «Opinion 4/2007 on the concept of personal data», som er en veileder til personopplysningsbegrepet etter direktiv 95/46, utdypes betydningen av hvert av de fire vilkårene i detalj.[38] Veilederen er skrevet av artikkel 29-gruppen som var en arbeidsgruppe sammensatt av representanter fra EU-landenes egne nasjonale datatilsyn og som hadde som formål å gi råd, veiledning og anbefalinger til EU-Kommisjonen med henhold til behandlingen av personopplysninger.[39]

En lignende gjennomgang av personopplysningsbegrepet har ikke blitt gjennomført av «European Data Protection Board» med henhold til GDPR, gruppen som erstattet artikkel 29-gruppen ved innføringen av GDPR. Følgelig vil utdypningen knyttet til direktiv 95/46 anvendes som tolkningsbidrag, da det må antas at bestemmelsene uansett må tolkes likt siden de har samme ordlyd. En slik forståelse er også støttet av Bygrave og Tosoni i deres artikkel i Oxford University Press sin kommentarutgave av GDPR.[40]

De fire vilkårene som artikkel 29-gruppen utdyper er sammenfallende med vilkårene man kan ekstrahere ut av den engelske bestemmelsens ordlyd. Disse er «any information», «relating to», «identified or identifiable» og «natural person».[41]

I den norske oversettelsen av GDPR brukes termen «om» hvor den engelske termen «related to» blir brukt. En mer direkte oversettelse kan imidlertid være «relatert til». Siden den eneste årsaken for at denne oppgaven bruker den uoffisielle norske oversettelsen av GDPR er for å øke lesbarheten av oppgaven, vil det i det følgende brukes den mer direkte oversettelsen «relatert til» i stedet for «om». Dette er for å i størst mulig grad ha vilkår som sammenfaller med den engelske offisielle versjonen, for å bedre kunne foreta en parallelltolkning av de engelske kildene på området. Se imidlertid delkapittel 5.3.1.3 hvor vilkåret behandles og varierende ordlyd på tvers av språkene problematiseres.

[38] Article 29 Data Protection Working Party, «Opinion 4/2007 on the concept of personal data», 20. juni 2007
[39] Se direktiv 95/46/EF artikkel 29
[40] Chrstioher Kuner, Lee A. Bygrave og Christopher Docksey, «The EU General Data Protection Regulation (GDPR) A Commentary», Oxford University Press 2020, s. 109
[41] Opinion 4/2007, s. 6.

Dette medfører at de fire vilkårene som utpensles av artikkel 29-gruppen og som vil danne strukturen for den nærmere vurderingen av om det på Bitcoin-nettverket behandles «personopplysninger», er følgende:

- «enhver opplysning»
- «relatert til»
- «en identifisert eller identifiserbar»
- «fysisk person»

5.3.1.1 «Enhver opplysning»

Det første som må vurderes er om data knyttet til en lommeboks transaksjonshistorikk og balanse er å anse som «enhver opplysning».

En naturlig språklig forståelse av «enhver opplysning» tilsier at vilkåret er ment å favne ekstremt vidt. Det er dermed tilstrekkelig at det er tale om en opplysning, da termen «enhver» ikke oppstiller noe videre begrensning. Videre må transaksjonshistorikk og en lommeboks balanse klart anses som en opplysning, da dataen er egnet til å opplyse om ny informasjon. Bestemmelsens ordlyd taler dermed for at informasjonen lagret på Bitcoin-nettverket må anses som «enhver opplysning».

En slik forståelse av at vilkåret er ment å favne vidt er også støttet i Nowak-dommen hvor EU-domstolen, med henhold til «enhver opplysning», uttalte at begrepet «reflects the aim of the EU legislature to assign a wide scope to that concept, which is not restricted to information that is sensitive or private, but potentially encompasses all kinds of information, not only objective but also subjective, in the form of opinions and assessments, provided that it 'relates' to the data subject».[42]

Vilkårets vidtrekkende karakter blir videre støttet av artikkel 29-gruppen hvor det understrekes at vilkåret har som formål å omfatte all form for informasjon.[43]

Ettersom både bestemmelsens ordlyd, samt øvrige rettskilder på området understreker at vilkåret er ment å favne vidt, er det uproblematisk å konstatere at informasjon om en digital lommeboks transaksjonshistorikk og balanse er å anse som «enhver opplysning». Vilkåret er i sin karakter ikke ment å være begrensende og er dermed klart oppfylt.

[42] Sak C-434/16, *Peter Nowak mot Data Protection Commissioner*, lagret i elektronisk samling for desember 2017, avsnitt 34.
[43] Opinion 4/2007 s. 6

5.3.1.2 «Fysisk Person»

Det neste vilkåret er om Bitcoin-nettverket behandler informasjon om en **«**fysisk person**».** En naturlig språklig forståelse av vilkåret tilsier at vilkåret tar sikte på å avgrense mot at forordningen kommer til anvendelse ved behandling av data som omhandler juridiske rettssubjekt slik som selskap, foreninger, stiftelser og lignende. En slik forståelse støttes også av artikkel 29-gruppen og legges følgelig til grunn.[44]

Det er på det rene at Bitcoin blir brukt av fysiske personer og at det lagres informasjon om dem. Vilkåret om «fysisk person» er følgelig oppfylt.

5.3.1.3 «Relatert til»

Videre oppstilles det et krav om opplysningen er **«relatert til»** et individ. Det må dermed vurderes om informasjon om en lommeboks balanse og transaksjonshistorikk må anses å være «relatert til» et individ slik at vilkåret er oppfylt.

En alminnelig språklig forståelse av «relatert til» tilsier at vilkåret oppstiller et krav om at opplysningen må ha en viss tilknytning til en person. Videre tilsier ordlyden av «relatert til» at også indirekte tilknytning kan være tilstrekkelig. Av den danske versjonen av GDPR, som også er offisiell, fremgår imidlertid en noe annen formulering enn hva som fremgår av den engelske. Her fremgår det at «I denne forordning forstås ved: »personoplysninger«: enhver form for information om en […] person». Ordlyden av informasjon «om» en person kan gi uttrykk for en mer restriktiv rekkevidde av vilkåret, da det kan tilsi et krav om at informasjonen må ha en direkte forbindelse med en person. Siden informasjon om en digital lommebok ikke omhandler en person direkte og at de offisielle versjonene av GDPR ikke gir et klart bilde med henhold til om indirekte forbindelse er tilstrekkelig, gir bestemmelsens ordlyd ikke en opplagt løsning på om informasjon om en digital lommebok på Bitcoin-nettverket er å anse som «relatert til» et individ. Vurderingen må følgelig bero på øvrige rettskilder på området.

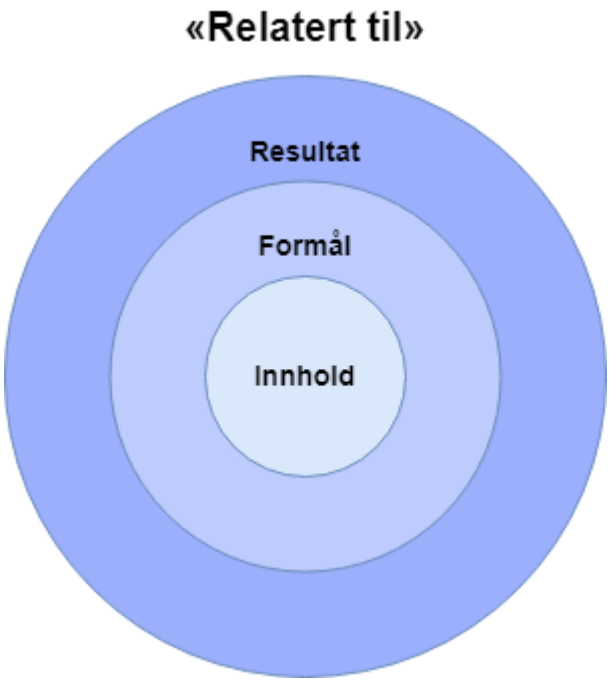
Rekkevidden av vilkåret «relatert til» blir nærmere behandlet av artikkel 29-gruppen i veilederen om personopplysninger. Her støttes forståelsen om at indirekte informasjon også kan innfri vilkåret om å være «relatert til» et individ.[45] Deretter presenterer veilederen følgende avsnitt om vilkårets rekkevidde:

[44] Ibid, s. 21-22 og s. 23-23
[45] Ibid, s. 9

> «In view of the cases mentioned above, and along the same lines, it could be pointed out that, in order to consider that the data “relate” to an individual, a "content" element OR a "purpose" element OR a "result" element should be present.»[46]

Utsagnet gir uttrykk for at vilkåret om å være «relatert til» et individ er oppfylt ved tilstedeværelsen av ett av tre alternative elementer. Disse elementene er «innhold», «formål» og «resultat».

Rekkevidden av vilkåret «relatert til» illustreres i figuren nedenfor. I denne figuren gir helheten av sirklene uttrykk for vilkårets rekkevidde. I midten finner man sirkelen som illustrer rekkevidden av elementet «innhold». Dersom dette elementet ikke er oppfylt kan man forflytte seg til sirkelens neste steg og vurdere om elementet «formål» er til stedet. Ytterst i sirkelen finner man elementet «resultat». Dersom heller ikke dette elementet er til stede, er man utenfor «relatert til» sin rekkevidde og vilkåret er følgelig ikke oppfylt.



Figur 6 - Visuell presentasjon av rekkevidden til vilkåret "relatert til"

Det første som må vurderes er om informasjon om en digital lommeboks balanse og transaksjonshistorikk må anses å være relatert til et individ som følge av tilstedeværelsen av elementet «innhold».

[46] Ibid, s. 10

Elementet «innhold» er ifølge artikkel 29-gruppen den meste direkte formen for å være «relatert til» da det omfatter den meste naturlige fortolkning av å være relatert til noe. For at informasjon skal være «relatert til» et individ som følge av «innhold»-elementet, må informasjonen være «om» individet.[47] For eksempel vil informasjon om Peder Ås sine fysiske trekk, bostedsadresse, medisinske historikk og inntekt klart være relatert til Peder, da informasjonen i sitt innhold handler om Peder.

Spørsmålet blir følgelig om informasjon om en digital lommeboks balanse og transaksjonshistorikk handler om en person.

Dette spørsmålet må besvares avkreftende. Det er klart at informasjon om en digital lommebok ikke omhandler en person, da det omhandler en digital lommebok. Informasjonen lagret på Bitcoin-nettverket kan følgelig ikke anses å være «relatert til» et individ basert på innholdselementet.

Det neste elementet som må vurderes er om informasjonen som er lagret på Bitcoin-nettverket må anses å være relatert til et individ som følge av tilstedeværelsen av elementet «formål». Dette er det andre nivået i figur 6 og ved oppfyllelse av dette elementet, vil man være innenfor rekkevidden av vilkåret «relatert til», til tross for at elementet «innhold» ikke er til stede.

Artikkel 29-gruppen presenterer «formål» som et element som ved oppfyllelse vil medføre at informasjonen er indirekte «relatert til» et individ. En slik indirekte relasjon kan oppstå når informasjonen ikke er direkte om et individ, men hvor individet har en tilstrekkelig tilknytning til det informasjonen retter seg mot. En slik tilknytning kan f.eks. være eierskap eller innflytelse, samt fysisk eller geografisk nærhet til et individ.[48]

Artikkel 29-gruppen utdyper innholdet i elementet videre i følgende avsnitt:

> «That "purpose" element can be considered to exist when the data are used or are likely to be used, taking into account all the circumstances surrounding the precise case, with the purpose to evaluate, treat in a certain way or influence the status or behaviour of an individual.»[49]

[47] Ibid, s. 10.
[48] Ibid, s. 9.
[49] Ibid, s. 10.

Elementet tar følgelig sikte på å omfatte situasjoner hvor informasjonen ikke er direkte om et individ, men hvor formålet med informasjonen er å evaluere, behandle eller påvirke et individ.

Man kan belyse denne forståelsen ved hjelp av et eksempel som knytter seg til lagret informasjon om Peder Ås sitt hus. Det første man kan konstatere er at elementet «innhold» ikke er til stede ettersom informasjonen ikke handler om Peder, men om huset. Hvis det har seg slik at formålet med å lagre informasjonen om huset er å kartlegge verdiutviklingen av nabolaget, kan heller ikke elementet «formål» være til stede og man er dermed i utgangspunktet utenfor rekkevidden av GDPR da informasjonen ikke er «relatert til» Peder. Akkurat den samme lagrede informasjonen kan imidlertid medføre at «formål» elementet er til stede, dersom formålet med lagringen av informasjonen er å avgjøre hvor mye Peder er pålagt å betale i skatt. Man er da innenfor GDPR sin rekkevidde da formålet med informasjonen om huset er å evaluere Peders skatterettslige posisjon.

Det må dermed foretas en vurdering av om informasjon om en digital lommeboks balanse og transaksjonshistorikk har som formål å evaluere, behandle eller påvirke et individ. Dersom det er tilfelle, vil elementet «formål» være til stede og følgelig må vilkåret «relatert til» anses oppfylt.

For å drifte en kryptovaluta er det nødvendig å lagre informasjon om balansene på lommebøkene og transaksjonene som foretas. Dette er en forutsetning for å kunne holde styr på verdiene i nettverket. Formålet med å lagre informasjon om lommebøkene og den tilhørende transaksjonshistorikken på Bitcoin-nettverket er dermed å gjøre det mulig å drifte kryptovalutaen. Dette medfører at elementet «formål» ikke er til stede, da formålet ikke knytter seg til et individ. Vilkåret om å være «relatert til» et individ kan følgelig ikke anses oppfylt basert på formålselementet.

Den tredje og siste steget er å vurdere om resultatelementet er til stede. Dette er det tredje nivået i figur 6. Dette elementet kan innfri vilkåret om å være «relatert til» et individ selv når informasjonen, verken i sitt innhold eller formål, omhandler en person. Dette elementet tar dermed sikte på å være en sikkerhetsventil for situasjoner hvor informasjonen sannsynligvis vil resultere i å påvirke et individ.[50]

Artikkel 29-gruppen utleder følgende om elementet:

[50] Ibid, s. 11.

> «Despite the absence of a "content" or "purpose" element, data can be considered to "relate" to an individual because their use is likely to have an impact on a certain person's rights and interests, taking into account all the circumstances surrounding the precise case. It should be noted that it is not necessary that the potential result be a major impact. It is sufficient if the individual may be treated differently from other persons as a result of the processing of such data.»[51]

Dette tilsier at elementet er ment å fange opp situasjoner hvor informasjonen som er lagret, verken i sitt innhold eller formål er om et individ, men hvor informasjonen likevel er egnet til å ha en innvirkning på individer.

En situasjon hvor dette resultatelementet kan lede til at vilkåret om å være «relatert til» innfris, kan belyses med et fiktivt eksempel med utgangspunkt i et taxiselskap. Dersom et taxiselskap lagrer sanntidsinformasjon om hvor enhver av selskapets taxier befinner seg under kjøring, er dette informasjon som i sitt innhold omhandler en gjenstand, da det er plasseringen av bilen som lagres. Videre er formålet med denne lagringen å optimalisere driften, da informasjon om plasseringen av hver bil kan gi selskapet et bedre beslutningsgrunnlag for å allokere den nærmeste bilen til ethvert oppdrag. Verken elementet «innhold» eller «formål» er dermed til stede, og følgelig er informasjonen i utgangspunktet ikke «relatert til» et individ. Det er her elementet «resultat» fungerer som en sikkerhetsventil for lagret data. Denne informasjonen har potensialet til å påvirke taxisjåførene. Informasjonen kan for eksempel brukes til å avgjøre hvilken av sjåførene som ikke respekterer fartsgrenser, hvem som er mest effektive og hvem som kaster bort mest tid gjennom unødig lange pauser. Den lagrede dataen må dermed anses å være «relatert til» enkeltindivider, da den har potensialet til å ha en innvirkning på taxisjåførene. [52]

Det må dermed vurderes om lagret informasjon om lommebøkers balanse og transaksjonshistorikk sannsynligvis vil ha en innvirkning på individers rettigheter og interesser. Dersom det er tilfelle vil elementet «resultat» være til stede noe som medfører at vilkåret om å være «relatert til» et individ er oppfylt.

Det er kun én måte å få tilgang til verdiene som er lagret på en digital lommebok og det er ved å ha kjennskap til lommebokens private nøkkel. Dette er en kode som blir opprettet i det man oppretter lommeboken, og som må holdes skjult dersom man ikke ønsker at andre skal kunne

[51] Ibid.
[52] Ibid

råde over verdiene lagret i lommeboken. Man står dermed ovenfor et tilfelle hvor det i utgangspunktet kun er personen som har opprettet lommeboken som har tilgang til den. Dette medfører at hver lommebok har en tilknytning til det individet som opprettet lommeboken, da det kun er dette individet som kan råde over verdiene.

Når det er en så stor tilknytning mellom den digitale lommeboken og individet som har tilgang til den, kan informasjon om en lommeboks balanse og transaksjonshistorikk anses å være sammenfallende med informasjon om eierens balanse og transaksjonshistorikk. Videre vil kjennskap til et individs økonomiske situasjon kunne brukes til å påvirke individets rettigheter og interesser. Det er dermed klart at informasjon om digitale lommebøkers balanse og transaksjonshistorikk vil sannsynligvis ha en innvirkning på individer forutsatt at individet er identifisert, noe som er det neste vilkåret som skal vurderes. Det må dermed legges til grunn at elementet «resultat» er til stede.

Siden ett av de tre alternative elementene er til stede, må det følgelig konkluderes med at vilkåret om å være «relatert til» et individ er oppfylt.

5.3.1.4 «Identifisert eller identifiserbar»

Det fjerde og siste vilkåret for at det skal være tale om en personopplysning er at dataen må være relatert til **«**en identifisert eller identifiserbar**»** person. Det må dermed vurderes om informasjonen som lagres på Bitcoin sin blokkjede omhandler «en identifisert eller identifiserbar» person.

Det første som kan konstateres ut ifra bestemmelsens ordlyd, er at det ikke er noe krav om at personen allerede har blitt identifisert, da det er tilstrekkelig at personen er «identifiserbar». Dersom en person allerede har blitt identifisert, er det klart at personen også må være identifiserbar. Det er av den grunn det det sistnevnte alternativet som i praksis har en betydning for hvorvidt vilkåret er oppfylt og som derfor vil være hovedfokuset for utdypningen videre.

En naturlig språklig forståelse av «identifiserbar» tilsier at det må foreligge en mulighet for at et individ kan bli «identifisert». Rekkevidden av om et individ er «identifiserbar» er dermed avhengig av hva det vil si at noen er identifisert. Det må derfor ses nærmere på hva det vil si å være «identifisert».

En naturlig språklig forståelse av at et individ er «identifisert» tilsier at man må ved hjelp av tilgjengelig informasjon klarer å si med sikkerhet hva som er identiteten til individet. For

eksempel tilsier dette at Satoshi Nakamoto vil være identifisert når man klarer å si med sikkerhet hva som er identiteten til personen(e) bak pseudonymet.

Det er ingen bestemmelse etter GDPR som behandler når et individ er å anse som «identifisert». Det må dermed ses hen til øvrige rettskilder på området.

Med henhold til «identifisert»-vilkåret kommer artikkel 29-gruppen med følgende utsagn:

> «In general terms, a natural person can be considered as "identified" when, within a group of persons, he or she is "distinguished" from all other members of the group. Accordingly, the natural person is "identifiable" when, although the person has not been identified yet, it is possible to do it (that is the meaning of the suffix "-able"). This second alternative is therefore in practice the threshold condition determining whether information is within the scope of the third element.»[53]

Her fremgår det at en person vil være identifisert når man har lykkes med å skille personen ut fra resten av en gruppe. Dette medfører at informasjon som anses å være tilstrekkelig til å gjøre en person «identifisert» vil variere fra situasjon til situasjon. For eksempel vil informasjon om en persons fornavn til vanlig ikke være tilstrekkelig dersom det er tale om en liste over alle som bor i Norge, men dersom det er en liste over elever i en klasse, vil situasjonen være ulik. Ettersom denne forståelsen samsvarer med hva som kan ekstraheres av vilkårets ordlyd, samt at vilkåret ikke blir behandlet nærmere i øvrige bestemmelser etter GDPR, legges det til grunn at et individ er «identifisert» når man kan skille personen ut fra resten av gruppen.

Alle opplysningene lagret på Bitcoin-nettverket er knyttet til et individ gjennom en adressekode tilknyttet deres digitale lommebok. Det må dermed vurderes om en spesifikk eier av en digital lommebok må anses å være «identifiserbar» som følge av at det vil være mulig å skille personen ut fra øvrige lommeboksholdere basert på tilgjengelig informasjon.

I GDPR artikkel 4 punkt 1 presenteres legaldefinisjonen av en personopplysning, videre utledes det også hva det vil si å være identifiserbar. Her fremgår det at:

> «en identifiserbar fysisk person er en person som direkte eller indirekte kan identifiseres, særlig ved hjelp av en identifikator, f.eks. et navn, et identifikasjonsnummer, lokaliseringsopplysninger, en nettidentifikator eller ett eller

[53] Ibid, s. 12.

> flere elementer som er spesifikke for nevnte fysiske persons fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sosiale identitet».

Første del av bestemmelsens ordlyd konstaterer at en identifiserbar person er en person som kan identifiseres, enten direkte eller indirekte. Videre fremgår det at identifikasjon ofte gjennomføres ved hjelp av en identifikator før det presenteres eksempler på slike identifikatorer. Hva som er å anse som en identifikator blir ikke videre utdypet, men basert på eksemplene som presenteres, tilsier bestemmelsen at en identifikator er informasjon som er egnet til å identifisere et individ.

I artikkel 29-gruppens veileder for personopplysninger, utledes følgende:

> «Identification is normally achieved through particular pieces of information which we may call "identifiers" and which hold a particularly privileged and close relationship with the particular individual.»[54]

Dette utsagnet tilsier at identifikatorer er informasjon som har en nær tilknytning til et individ og som dermed kan bidra til å identifisere et individ. Denne forståelsen samsvarer ordlydstolkningen av bestemmelsen og legges dermed til grunn.

Med henhold til Bitcoin-nettverket er det to kilder til informasjon som kan bidra til å identifisere et individ og som følgelig må anses som «identifikatorer». Dette er hver lommeboks offentlige adresse og lommebokens tilhørende økonomiske data, hvor sistnevnte innebærer både lommebokens transaksjonshistorikk og den nåværende økonomiske balansen. Vurderingen av om individene på Bitcoin-nettverket er identifiserbare må dermed tas på grunnlag av disse identifikatorene.

Hvis man tar utgangspunkt i transaksjonen i figur 4, ser man at det ikke lagres informasjon som identifiserer individene i transaksjonen. Adressekoden er en helt tilfeldig generert kode som ikke har noe tilknytning til individenes identitet. Basert på informasjonen lagret i transaksjonen kan man kun se at det er foretatt en transaksjon, men hvem det er som har foretatt transaksjonen er det ikke mulig å vite. Dette tilsier at individene ikke er «identifiserbare».

I fortalepunkt 26 utdypes imidlertid rekkevidden av vilkåret «identifiserbar» hvor følgende utdrag kan hentes:

[54] Ibid.

> «Når det skal fastslås om en fysisk person er identifiserbar, bør det tas hensyn til alle midler som det med rimelighet kan tenkes at den behandlingsansvarlige eller en annen person kan ta i bruk for å identifisere vedkommende direkte eller indirekte, f.eks. utpeking. For å fastslå om midler med rimelighet kan tenkes å bli tatt bruk for å identifisere den fysiske personen 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.»

Utdraget gir uttrykk for at i vurderingen av om et individ må anses å være identifiserbart må det foretas en helhetlig vurdering av om det foreligger midler som det med rimelighet kan tenkes at noen kan bruke for å identifisere individet.

I Bitcoin sitt tilfelle kan personer kombinere sine egne observasjoner med transaksjonsinformasjonen som lagres på Bitcoin-nettverket for å identifisere individene bak adressekodene. Dette kan illustreres ved hjelp av et eksempel. Dersom Peder og Hans er ute og spiser, og Peder bestemmer seg for å betale med Bitcoin, kan Hans senere finne Peder sin digitale lommebok dersom han noterer seg hvor mye måltidet kostet og klokkeslett for betalingen. Hans kan deretter søke gjennom alle transaksjonene og finne en match for riktig tidspunkt og riktig beløp. På denne måten har Hans klart å knytte Peder sin digitale lommebok til Peder ved hjelp av tilleggsopplysningene som Hans innehar. Et slikt søk er også noe man rimelighet kan kunne forvente at brukes, ettersom nettbaserte hjelpemidler som Blockchair.com sitt transaksjonssøk gjør det svært enkelt å gjennomføre.[55]

Dette medfører at individene på Bitcoin-nettverket må anses som «identifiserbare» da det med tilleggsopplysninger som det med rimelighet må forventes å brukes, vil være mulig å finne ut hvem det er som er innehaveren av en digital lommebok. Det siste vilkåret om at dataen må være relatert til «en indentifisert eller identifiserbar» person er følgelig også oppfylt. Dette medfører at det på Bitcoin nettverket behandles «personopplysninger».

Følgelig foregår det «helt eller delvis automatisert» «behandling» av «personopplysninger» på Bitcoin-nettverket. Bitcoin er dermed innenfor GDPR sitt materielle anvendelsesområde.

[55] https://blockchair.com/bitcoin/transactions

5.4 Konklusjon av om GDPR kommer til anvendelse på Bitcoin

Som følge av at Bitcoin oppfyller vilkårene for GDPR sitt geografiske og materielle anvendelsesområde, behandlet i henholdsvis delkapittel 5.2 og 5.3, konkluderes det følgelig med at forordningen kommer til anvendelse på kryptovalutaen. Dette medfører at Bitcoin er pliktig til å overholde kravene som oppstilles etter GDPR.

6. Opererer Bitcoin i strid med GDPR som følge av brudd på retten til å bli glemt

6.1 Presentasjon av retten til å bli glemt

Nå som det har blitt konstatert at GDPR kommer til anvendelse på Bitcoin, er det neste steget å vurdere om Bitcoin oppfyller kravene som fremgår av GDPR. I avsnitt 3 i forordningen kalt «den registrertes rettigheter» utpensles det en rekke rettigheter som den registrerte innehar og som den ansvarlige plikter å kunne ivareta. I det følgende vil retten til sletting etter artikkel 17 problematiseres for å avgjøre om Bitcoin kan ivareta denne rettigheten. Dersom denne rettigheten ikke kan ivaretas medfører det at kryptovalutaen opererer i strid med GDPR.

GDPR artikkel 17 første ledd har følgende ordlyd:

> «1. Den registrerte skal ha rett til å få personopplysninger om seg selv slettet av den behandlingsansvarlige uten ugrunnet opphold, og den behandlingsansvarlige skal ha plikt til å slette personopplysninger uten ugrunnet opphold dersom et av de følgende forhold gjør seg gjeldende:
>
> a. personopplysningene er ikke lenger nødvendige for formålet som de ble samlet inn eller behandlet for,
>
> b. den registrerte trekker tilbake samtykket som ligger til grunn for behandlingen, i henhold til artikkel 6 nr. 1 bokstav a) eller artikkel 9 nr. 2 bokstav a), og det ikke finnes noe annet rettslig grunnlag for behandlingen,
>
> c. den registrerte protesterer mot behandlingen i henhold til artikkel 21 nr. 1, og det ikke finnes mer tungtveiende berettigede grunner til behandlingen, eller den registrerte protesterer mot behandlingen i henhold til artikkel 21 nr. 2,
>
> d. personopplysningene er blitt behandlet ulovlig,

e. personopplysningene må slettes for å oppfylle en rettslig forpliktelse i unionsretten eller medlemsstatenes nasjonale rett som den behandlingsansvarlige er underlagt,

f. personopplysningene er blitt samlet inn i forbindelse med tilbud om informasjonssamfunnstjenester som nevnt i artikkel 8 nr. 1

2. […]

3. Nr. 1 og 2 får ikke anvendelse dersom nevnte behandling er nødvendig

a. for å utøve retten til ytrings- og informasjonsfrihet,

b. for å oppfylle en rettslig forpliktelse som krever behandling i henhold til unionsretten eller medlemsstatenes nasjonale rett som den behandlingsansvarlige er underlagt, eller for å utføre en oppgave i allmennhetens interesse eller utøve offentlig myndighet som den behandlingsansvarlige er pålagt,

c. av hensyn til allmennhetens interesse på området folkehelse i samsvar med artikkel 9 nr. 2 bokstav h) og i) og artikkel 9 nr. 3,

d. for arkivformål i allmennhetens interesse, for formål knyttet til vitenskapelig eller historisk forskning eller for statistiske formål i samsvar med artikkel 89 nr. 1 i den grad rettigheten nevnt i nr. 1 sannsynligvis vil gjøre det umulig eller i alvorlig grad vil hindre at målene med nevnte behandling nås, eller

e. for å fastsette, gjøre gjeldende eller forsvare rettskrav»

En naturlig språklig forståelse av at den registrerte «skal ha rett til» å få personopplysninger om seg selv slettet tilsier at bestemmelsen oppstiller den registrerte en mulighet til å få personopplysningene slettet. Denne rettigheten oppstår dersom et av alternativene utpenslet fra a til f er oppfylt. Videre er en rettighet tosidet; på den ene siden oppstilles det en mulighet for rettighetshaveren, på den andre siden oppstilles det en plikt for motparten som i dette tilfellet er den behandlingsansvarlige. Bestemmelsens ordlyd gir dermed uttrykk for at dersom den behandlingsansvarlige ikke er i stand til å gjennomføre slettingen, vil deres behandling av personopplysninger i utgangspunktet være i strid med plikter som oppstilles etter GDPR. Unntak fra dette utgangspunktet fremgår av bestemmelsens tredje ledd.

Som presentert i avsnitt 4.3 opererer Bitcoin på blokkjedeteknologi, en form for database som er uforanderlig av design. Når informasjon først har blitt lagt til i blokkjeden vil det være svært vanskelig å slette denne informasjonen. Her oppstår det dermed et spenningsforhold mellom kryptovalutaen og GDPR som skal undersøkes nærmere. I det følgende vil det først vurderes om et av vilkårene utpenslet i GDPR artikkel 17 første ledd alternativ a til f er innfridd, deretter vil rekkevidden av vilkåret «slettet» utpensles før det vil vurderes om Bitcoin evner å foreta en slik sletting. Til slutt vil det vurderes om Bitcoin oppfyller et av unntakene fra rettigheten etter bestemmelsens tredje ledd.

6.2 Alternativene a til f etter GDPR artikkel 17 første ledd

Det skal nå vurderes om det i tilfelle av Bitcoin innfris ett av de seks alternative vilkårene slik at den registrerte innehar retten til å bli glemt etter GDPR artikkel 17 første ledd. Det er ett alternativ som er relevant i denne sammenheng og som skal ses nærmere på. Dette er alternativ b som har følgende ordlyd:

> «den registrerte trekker tilbake samtykket som ligger til grunn for behandlingen, i henhold til artikkel 6 nr. 1 bokstav a) eller artikkel 9 nr. 2 bokstav a), og det ikke finnes noe annet rettslig grunnlag for behandlingen»

Bestemmelsen gir uttrykk for at dersom det er samtykke som er det eneste grunnlaget for behandlingen av personopplysninger, vil den registrerte inneha en rett til å trekke samtykket tilbake og dermed få sine personopplysninger slettet.

Det må dermed vurderes om det er samtykke som er det eneste grunnlaget for Bitcoin sin behandling av personopplysninger slik at de registrerte kan gjøre sin rett til å bli glemt gjeldende med grunnlag i å trekke sitt samtykket tilbake.

Av GDPR artikkel 6 om behandlingens lovlighet, fremgår det i bestemmelsens første ledd det følgende:

> «Behandlingen er bare lovlig dersom og i den grad minst ett av følgende vilkår er oppfylt:
>
> a. den registrerte har samtykket til behandling av sine personopplysninger for ett eller flere spesifikke formål,

b. behandlingen er nødvendig for å oppfylle en avtale som den registrerte er part i, eller for å gjennomføre tiltak på den registrertes anmodning før en avtaleinngåelse,

c. behandlingen er nødvendig for å oppfylle en rettslig forpliktelse som påhviler den behandlingsansvarlige,

d. behandlingen er nødvendig for å verne den registrertes eller en annen fysisk persons vitale interesser,

e. behandlingen er nødvendig for å utføre en oppgave i allmennhetens interesse eller utøve offentlig myndighet som den behandlingsansvarlige er pålagt,

f. behandlingen er nødvendig for formål knyttet til de berettigede interessene som forfølges av den behandlingsansvarlige eller en tredjepart, med mindre den registrertes interesser eller grunnleggende rettigheter og friheter går foran og krever vern av personopplysninger, særlig dersom den registrerte er et barn»

Bestemmelsen gir uttrykk for en uttømmende liste over behandlingsgrunnlagene som kan ligge til grunn for at behandling av personopplysninger skal være lovlig. Ingen av alternativene fra b til f er relevant i Bitcoin sitt tilfelle. Behandlingen må følgelig begrunnes i samtykke etter bestemmelsens bokstav a for at behandling skal være lovlig.

Bitcoin behandler utelukkende personopplysningene til individer som har valgt å delta i nettverket ved å besitte verdier i Bitcoin. Nevnte personopplysninger er transaksjonshistorikk og lommebokbalanse, noe som er nødvendig data for å drifte en kryptovaluta. Behandlingen av personopplysningene har dermed et spesifikt formål. Dette tilsier at det er treffende å anse Bitcoin sitt behandlingsgrunnlag som samtykke etter GDPR artikkel 6 første ledd punkt a.

Dette inviterer til en drøftelse av om det foreligger et gyldig samtykke etter GDPR artikkel 7. Dette vil imidlertid ikke behandles da oppgavens problemstilling oppstiller spørsmål om det foreligger brudd på GDPR som følge av brudd på retten til å bli glemt og ikke på grunnlag av samtykkets gyldighet. I det følgende vil det dermed forutsettes at det foreligger et gyldig samtykke etter GDPR artikkel 7.

Det legges dermed til grunn at Bitcoin sitt behandlingsgrunnlag er samtykke etter GDPR artikkel 6 punkt a da individene har valgt å delta i nettverket.

Som følge av at grunnlaget for behandlingen er samtykke etter GDPR artikkel 6 første ledd punkt a, medfører dette at de registrerte innehar en rett til å trekke tilbake dette samtykket og få sine personopplysninger slettet etter GDPR artikkel 17 første ledd punkt b, gitt at «det ikke finnes noe annet rettslig grunnlag for behandlingen». Siden samtykke er det eneste treffende behandlingsgrunnlaget, foreligger det ingen andre rettslige grunnlag for behandlingen. Dette medfører at minst ett av de alternative vilkårene a til f er oppfylt og følgelig innehar den registrerte retten til å bli glemt etter GDPR artikkel 17 første ledd.

6.3 Rekkevidden av «slettet» etter GDPR artikkel 17

Ettersom minst ett av de seks alternative vilkårene fra a til f er oppfylt, medfører dette at de registrerte på Bitcoin-nettverket i utgangspunktet har en rettighet til å få sine personopplysninger slettet. Dermed må rekkevidden av termen «slettet» kartlegges for å avgjøre om Bitcoin er i stand til å ivareta denne rettigheten, ved å opprettholde deres plikt til å slette data ved forespørsel.

En naturlig språklig forståelse av «slettet» tilsier at informasjonen må være fjernet eller tilintetgjort og følgelig ikke lenger tilgjengelig. I Bitcoin sitt tilfelle innebærer dette at all informasjon vedrørende transaksjonshistorikk og balanse knyttet til rettighetsutøverens digitale lommebok, blir fjernet fra blokkjeden.

I Nowak-saken utleder domstolen «it cannot be ruled out that a candidate may, under Article 12(b) of Directive 95/46, have the right to ask the data controller to ensure that his examination answers and the examiner's comments with respect to them are, after a certain period of time, erased, that is to say, destroyed».[56] Nevnte sak omhandlet imidlertid ikke retten til sletting, noe som medfører at uttalelsen må anses som et obiter dictum. Dommens prejudikatverdi er dermed begrenset. Likevel er dommen et sterkt argument for at «slettet» må forstås som «destroyed». Dette kan tilsi at vilkåret ikke er oppfylt før personopplysningene er fullstendig borte og at handlingen må være irreversibel. Også dette tilsier at Bitcoin må fjerne informasjon vedrørende rettighetsutøverens transaksjonshistorikk og balanse fra blokkjeden.

I Bitcoin sitt tilfelle vil det være svært vanskelig å fjerne personopplysningene fra blokkjeden slik at informasjonen ikke lenger er tilgjengelig. Siden blokkjeder henger sammen basert på blokkens hasjfunksjon, må alle blokkene datert etter den blokken man ønsker å slette informasjon fra endres. Dette er som følge av at ved en endring på en blokk tidligere i kjeden,

[56] Sak C-434/16, *Peter Nowak mot Data Protection Commissioner*, avsnitt 55

vil senere blokkere nå ha en utdatert hash ettersom hashen er basert på foregående blokkers informasjon. Man må derfor gjenbygge hele blokkjeden, blokk for blokk, helt tilbake til det tidspunktet hvor man vil gjennomføre endringen. Når det per dags dato er tale om hundretusenvis av blokker som inneholder tusenvis av transaksjoner hver, er det klart at dette er en komplisert oppgave.

Muligheten for å gjennomføre en slik endring minskes drastisk når man også tar stilling til Bitcoin sin konsensusprotokoll. Dersom endringen skal vedvare, må endringen oppnå konsensus i Bitcoin-nettverket. Hvis ikke vil Bitcoin-nettverket raskt identifisere noden som innehar blokkjeden som skiller seg ut ifra de andres og dermed ekskludere den. Den kompliserte endringen utpenslet i forrige avsnitt må dermed skje i flertallet av nodene samtidig, slik at endringen oppnår konsensus i nettverket. En slik endring er teoretisk mulig, men i praksis må det anses som en tilnærmet umulig oppgave å gjennomføre. Det må følgelig legges til grunn at Bitcoin ikke har en adgang til å fjerne personopplysninger som allerede er lagret på blokkjeden.

EU-domstolen har imidlertid akseptert alternative former for å oppfylle retten til å bli glemt. I Google Spain saken var spørsmålet om Google var pliktet å fjerne en artikkel fra Google-søkeresultater på grunnlag av retten til å bli glemt etter direktiv 95/46 artikkel 12 punkt b, som må anses som forgjengeren til blant annet GDPR artikkel 17. I dommens avgjørelse fremgår det at «the data subject may, by virtue of Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46, require those links to be removed from the list of results.»[57] Dette medfører at domstolen aksepterte fjerning fra søkemotorresultater som tilstrekkelig for å oppfylle vilkåret om «erasure».

Denne forståelsen ble videreført i CNIL mot Google hvor Google Spain saken blir referert. I dommens avsnitt 46, skrives det: «In the context of Regulation 2016/679, that right of a data subject to de-referencing is now based on Article 17 of that regulation, which specifically governs the 'right to erasure', also referred to, in the heading of that article, as the 'right to be forgotten'.»[58]

Det må likevel konstateres at Google, med henhold til Google Spain saken, selv ikke hadde tilgang til den opprinnelige artikkelen og at de dermed ikke hadde mulighet til å gjennomføre en tradisjonell form for sletting. Videre var fjerning fra søkemotorresultater det eneste

[57] Sak C-131/12, *Google Spain mot AEPD og Mario Costeja González*, Avsnitt 98.
[58] Sak C-507/17, *Google mot CNIL*, avsnitt 46

saksøker krevde og dermed det eneste domstolen tok stilling til. Dommen kan dermed kun være en svak indikator på at alternative løsninger kan aksepteres for å oppfylle vilkåret «slettet».

Dette kan tilsi at vilkåret «slettet» har et større anvendelsesområde enn hva som fremgår av bestemmelsens ordlyd og antydningene presentert i Nowak-dommen. Det må dermed vurderes om det i Bitcoin sitt tilfelle foreligger alternative løsninger som kan innfri vilkåret om «slettet».

I analysen «Can distributed ledgers be squared with European data protection law?» skrevet for European Parliamentary Research Service, presenteres en slik alternativ form for sletting i form av å destruere den private nøkkelen til den registrerte.[59] I mange nettverk basert på blokkjedeteknologi, blir ofte personopplysninger lagret kryptert på blokkjeden. For å få tilgang til informasjonen kreves det en privat nøkkel i form av en kode, som kan dekryptere dataen. Dersom denne private nøkkelen slettes slik at ingen lenger har tilgang til den, vil personopplysningene fortsatt være lagret på blokkjeden, men i et kryptert format som ikke lenger kan dekrypteres. En slik løsning kan oppfylle GDPR sitt krav om «slettet», men kan ikke anvendes med henhold til Bitcoin. Personopplysningene det er tale om er ikke skjult bak en privat nøkkel, og følgelig vil destruksjon av en registrert sin private nøkkel kun resultere i at ingen lenger vil kunne råde over den digitale lommeboken. Personopplysningene vil fortsatt være til stede i et ukryptert format på blokkjeden.

Det foreligger dermed ingen måte Bitcoin kan slette personopplysningene som er lagret på nettverket. Utgangspunktet blir følgelig at Bitcoin opererer i strid med GDPR da den ikke kan opprettholde deres plikt til å ivareta en registrert sin rett til å bli «slettet» etter GDPR artikkel 17 første ledd.

6.4 Unntaket etter GDPR artikkel 17 tredje ledd

Til tross for at Bitcoin ikke kan opprettholde de registrertes rett til å bli glemt etter GDPR artikkel 17 første ledd, kan kryptovalutaen likevel være i samsvar med GDPR dersom den oppfyller et av unntakene presentert i GDPR artikkel 17 tredje ledd.

Unntaksbestemmelsen i tredje ledd gir uttrykk for en uttømmende liste og har følgende ordlyd:

[59] Finck (2019), s. 76 og 77.

«Nr. 1 og 2 får ikke anvendelse dersom nevnte behandling er nødvendig

a. for å utøve retten til ytrings- og informasjonsfrihet,

b. for å oppfylle en rettslig forpliktelse som krever behandling i henhold til unionsretten eller medlemsstatenes nasjonale rett som den behandlingsansvarlige er underlagt, eller for å utføre en oppgave i allmennhetens interesse eller utøve offentlig myndighet som den behandlingsansvarlige er pålagt,

c. av hensyn til allmennhetens interesse på området folkehelse i samsvar med artikkel 9 nr. 2 bokstav h) og i) og artikkel 9 nr. 3,

d. for arkivformål i allmennhetens interesse, for formål knyttet til vitenskapelig eller historisk forskning eller for statistiske formål i samsvar med artikkel 89 nr. 1 i den grad rettigheten nevnt i nr. 1 sannsynligvis vil gjøre det umulig eller i alvorlig grad vil hindre at målene med nevnte behandling nås, eller

e. for å fastsette, gjøre gjeldende eller forsvare rettskrav»

Ingen av punktene i bestemmelsen er spesielt treffende med henhold til det å drifte en desentralisert valuta. Videre vil det at bestemmelsen gir uttrykk for at unntak fra hovedregelen om at registrerte har en rett til å bli glemt, sammenholdt med bestemmelsens nødvendighetskrav, tilsi at det er en høy terskel for å innfrielse. Følgelig legges det til grunn at Bitcoin ikke oppfyller noen av unntakene presentert etter GDPR artikkel 17 tredje ledd punkt a til e. Utgangspunktet om at de registrerte på Bitcoin-nettverket har en rett til å bli glemt blir følgelig stående.

6.5 Konklusjon av om Bitcoin opererer i strid med GDPR som følge av brudd på retten til å bli glemt

Det har nå blitt konstatert at de registrerte på Bitcoin-nettverket har en rett til å bli glemt etter GDPR artikkel 17 første ledd, at Bitcoin ikke evner å foreta en handling som tilfredsstiller kravet om «slettet» og at ingen av unntakene etter GDPR artikkel 17 tredje ledd gjør seg gjeldende. Dette medfører at Bitcoin ikke evner å ivareta registrertes rett til sletting og at kryptovalutaen følgelig opererer i strid med GDPR sine bestemmelser.

7. Konklusjon og avsluttende betraktninger

I denne oppgaven har det blitt forsøkt å besvare den overordnede problemstilling som ble presentert i delkapittel 1.1:

> «Er Bitcoin regulert av personvernforordningen og opererer kryptovalutaen i så fall i strid med forordningen som følge av dens manglende evne til å oppfylle brukernes rett til å bli glemt etter artikkel 17?»

Kapittel 5. i oppgaven tok for seg det første delspørsmålet i problemstillingen om GDPR kommer til anvendelse på Bitcoin. Oppgavens funn er at kryptovalutaen innfrir det geografiske anvendelsesområdet etter GDPR artikkel 3 annet ledd, da kryptovalutaen etter «targeting»-kriteriet må anses å sikte seg inn på brukere lokalisert innen EU.

Videre ble det vurdert om dataen som behandles på Bitcoin-nettverket må anses å være innenfor GDPR sitt materielle anvendelsesområde. Vilkåret som krevde en nærmere analyse var «personopplysninger» som presenteres i GDPR artikkel 2 første ledd. Særlig måtte det undersøkes om dataen på Bitcoin-nettverket var «relatert til» et individ, og hvorvidt individene på nettverket må anses som «identifiserbare» slik artikkel 29-gruppen presenter i opinion 4/2007.

Med henhold til vurderingen av om dataen på Bitcoin-nettverket er «relatert til» et individ, var funn at som følge av at det er en så nær tilknytning mellom informasjon vedrørende en digital lommebok og informasjon om eieren av den gitte lommeboken, medførte dette at «resultat»-kriteriet som utpenslet av artikkel 29-gruppen må anses å være til stede. Følgelig var konklusjonen at informasjonen som lagres på Bitcoin-nettverket må anses å være «relatert til» et individ.

Videre funn viste at eierne av de digitale lommebøkene må anses å være «identifiserbare», da det ved hjelp av tilleggsopplysninger er mulig å finne ut hvem som er eier av de forskjellige lommebøkene, siden all transaksjonsdata offentliggjøres med både tidspunkt og beløp på nettverket. Dersom man registrerer hvilket klokkeslett en person foretar en transaksjon og hvor mye betalingen er på, vil man i ettertid kunne søke gjennom transaksjonene og innsnevre søket basert på tilleggsopplysningene om tidspunkt og beløp for å finne ett treff.

Konklusjonen på første del av problemstillingen var dermed at Bitcoin innfrir alle vilkårene for både det geografiske og materielle anvendelsesområdet og at GDPR følgelig kommer til anvendelse på Bitcoin.

Den andre delen av problemstillingen tar for seg hvorvidt Bitcoin opererer i strid med GDPR sine bestemmelser som følge av kryptovalutaens manglende evne til å ivareta de registrertes rett til å bli glemt etter GDPR artikkel 17. Funn var at de registrerte innehar en rett til å bli glemt ettersom Bitcoin sitt behandlingsgrunnlag er samtykke etter GDPR artikkel 17 første ledd punkt a og at ingen av unntakene etter bestemmelsens tredje ledd gjorde seg gjeldende. Videre er det i praksis umulig å slette informasjon som er lagret på Bitcoin-nettverket, da lagringssystemet er basert på blokkjedeteknologi som er uforanderlig av karakter. Det er dermed ingen måte for Bitcoin å ivareta de registrertes rett til å bli glemt og at kryptovalutaen opererer følgelig i strid med GDPR artikkel 17.

Konklusjonen på problemstillingen blir dermed:

> «Bitcoin er regulert av personvernforordningen og dette medfører at kryptovalutaen opererer i strid med forordningen som følge av dens manglende evne til å oppfylle brukernes rett til å bli glemt etter artikkel 17.»

Denne konklusjonen åpner opp for en diskusjon rundt hva som er rettsvirkningen av at Bitcoin opererer i strid med GDPR. Som presentert i oppgavens kapittel 3. kan den behandlingsansvarlige etter GDPR artikkel 83 ilegges en forholdsmessig bot som skal virke avskrekkende på opptil 20 000 000 EUR. Men som nevnt under kapittel 5.2 er det ikke klart hvem som er behandlingsansvarlig på Bitcoin-nettverket.

Ved første øyekast ser det ut som at Bitcoin ikke har en behandlingsansvarlig da det tilsynelatende ikke er noen som «bestemmer formålet med behandlingen av personopplysninger og hvilke midler som skal benyttes» jf. GDPR artikkel 4 punkt 7. Dersom dette er tilfellet, vil det dermed ikke foreligge en behandlingsansvarlig som kan pålegges å betale boten.

Dersom man legger til grunn antydningene som fremgår av Finck (2019) og Rode (2019) om at det er tale om et delt behandlingsansvar mellom nodene på nettverket, vil det i praksis være problematisk å kreve inn gebyret.[60] Ansvaret vil være pulverisert mellom titusenvis av noder noe som gjør innkrevingsprosessen svært krevende.[61]

Problematikken rundt ileggelsen av bøter til behandlingsansvarlig på Bitcoin-nettverket avdekker et viktig spørsmål. Som nevnt er konklusjonen på denne oppgaven at GDPR

[60] Se kapittel 5.2
[61] Se https://bitnodes.io/nodes/all/ for oppdatert antall noder

kommer til anvendelse på Bitcoin og at kryptovalutaen opererer i strid med forordningen, men er dette lovgivers intensjon? GDPR er i stor grad utformet på en måte hvor det forutsettes at det er uproblematisk å fastslå hvem det er som er behandlingsansvarlig.[62] Dette er tilfelle for blant annet selskaper, foreninger og organisasjoner som alle opererer med et fastsatt styre, men for desentraliserte nettverk som Bitcoin er det mer usikkert. Kryptovaluta er fortsatt et svært nytt konsept og det er dermed ikke usannsynlig at lovgiver har på utilsiktet vis gitt GDPR en rekkevidde som også inkluderer kryptovalutaer. Kryptovalutaer blir ikke nevnt i GDPR, verken i bestemmelsene eller i fortalen og spenningen mellom kryptovalutaer og GDPR har heller ikke blitt behandlet i domstolen.

Om Bitcoin er i strid med forordningen, slik jeg har ønsket å sannsynliggjøre i oppgaven, er det betenkelig at en så stor digital tjeneste opererer helt uten motstand fra GDPR. Dersom det viser seg at konklusjonen er feil og at GDPR ikke regulerer kryptovaluta, er det betenkelig at forordningen er utformet på en måte hvor kryptovaluta tilsynelatende også omfattes. Det er dermed et behov for en avklaring av forholdet mellom kryptovalutaer og GDPR på EU-rettslig nivå.

[62] Se f.eks. behandling av det geografiske anvendelsesområdet i kapittel 5.2

8. Litteraturliste

8.1 Lover, traktater og forordninger

Personopplysningloven	Lov 15 juni 2018 nr. 38 om behandling av personopplysninger (personopplysningsloven)
EØS-loven	Lov 27 november 1992 nr. 109 om gjennomføring i norsk rett av hoveddelen i avtale om Det europeiske økonomiske samarbeidsområde (EØS-loven)
Personvernsforordningen	Europaparlaments- og rådsforordning (EU) 2016/679 av 27. april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger
ODA	Avtale av 2. mai 1992 mellom EFTA-statene om opprettelse av et overvåkningsorgan og en domstol, med protokollene 1 – 7 (ODA)
Menneskerettighetene	Europarådets konvensjon 4. november 1950 om beskyttelse av menneskerettighetene og de grunnleggende friheter som endret ved femtende protokoll 24. juni 2013
EU pakt om grunnleggende rettigheter	Den europeiske unions pakt om grunnleggenderettigheter av 1. desember 2009
Direktiv 95/46	Europaparlamentets og Rådets direktiv 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.

8.2 Rettspraksis

Sak C-434/16	Peter Nowak mot Data Protection Commissioner, 20. desember 2017
Sak C-131/12	Google Spain mot AEPD og Mario Costeja González, 13. mai 2014
Sak C-507/17	Google mot CNIL, 24. september 2019

HR-2021-966-A

8.3 Juridisk litteratur

8.3.1 Bøker

Johan Giertsen, «Avtaler», 4, utgave, Universitetsforlaget 2021

Chrstioher Kuner, Lee A. Bygrave og Christopher Docksey, «The EU General Data Protection Regulation (GDPR) A Commentary», Oxford University Press 2020

Finn Arnesen mfl., «Oversikt over EØS-retten», Universitetsforlaget 2022

8.3.2 Artikler

European Data Protection Board, «Guidelines 3/2018 on the territorial scope of the GDPR (Article 3)», 12. november 2019

Dr Michèle Finck, European Parliamentary Research Service, «Blockchain and the General Data Protection Regulation – Can distributed ledgers be squared with European data protection law?», juli 2019

Ane Victoria Rode, «Hvem er ansvarlig for personopplysninger i blokkjeder?», 10 desember 2019

Article 29 Data Protection Working Party, «Opinion 4/2007 on the concept of personal data», 20. juni 2007

8.6 Nettsider

Alle nettsidene er gjennomgått og oppdaterte per 05.12.2022.

Søk etter Bitcoin på NRK sine nettsider	https://www.nrk.no/sok/?q=Bitcoin
Statistisk sentralbyrå, «Fakta om internett og mobil»	https://www.ssb.no/teknologi-og-innovasjon/faktaside/internett-og-mobil
Nordea, «General Data Protection Regulation (GDPR)»	https://www.nordea.no/privat/kundeservice/general-data-protection-regulation.html
DnB, «DNBs personvernerklæring»	https://www.dnb.no/om-oss/personvern.html?la=NO&site=DNB_NO
Alex Hern, The Guardian, «Google fined record £44m by French data protection watchdog», 21 januar 2019	https://www.theguardian.com/technology/2019/jan/21/google-fined-record-44m-by-french-data-protection-watchdog
Forfatter ikke opplyst, BBC, «H&M fined for breaking GDPR over employee surveillance», 5. oktober 2020	https://www.bbc.com/news/technology-54418936
Carly Page, TechCrunch, «EU hits Amazon with record-breaking $887M GDPR fine over data misuse», 30. juli 2021	https://techcrunch.com/2021/07/30/eu-hits-amazon-with-record-breaking-887m-gdpr-fine-over-data-misuse/
Satoshi Nakamoto, «Bitcoin: A Peer-to-Peer Electronic Cash System», oktober 2008	https://bitcoin.org/en/bitcoin-paper

Markedsverdi hentet fra Coinmarketcap	https://coinmarketcap.com/currencies/bitcoin/
Connor Murray, «The mystery of the Genesis block», Coingeek, 7. desember 2021	https://coingeek.com/the-mystery-of-the-genesis-block/
Jake Frankenfield, «Cryptocurrency Explained With Pros and Cons for Investment», Investopedia, 26. september 2022	https://www.investopedia.com/terms/c/cryptocurrency.asp
Adam Hayes, «Blockchain Facts: What Is It, How It Works, and How It Can Be Used», Investopedia, 27. september 2022	https://www.investopedia.com/terms/b/blockchain.asp
Forfatter ikke opplyst, «Cryptography Hash Functions», Tutorialspoint, uten år	https://www.tutorialspoint.com/cryptography/cryptography_hash_functions.htm
Lenke til info om blokk 758892 som brukes som eksempel	https://www.blockchain.com/explorer/blocks/btc/758892
Lenke til Blockchair sitt verktøy for transaksjonssøk	https://blockchair.com/bitcoin/transactions
Lenke til oppdaterte tall for antall noder på Bitcoin-nettverket	https://bitnodes.io/nodes/all/

9. Liste over figurer