Dataveileder for samferdselssektoren

– Veileder for deling av personopplysninger og andre data i samferdselssektoren

Versjon 1.0
Oppdatert 27.04.2026

Innholdsfortegnelse

0. Veilederens utforming 3

1 Om veilederen 3

1.1 Bakgrunn og formål 3

1.2 Verdien av å dele data 4

1.3 Forholdet til nasjonal lovgivning og sektorlovgivningen 4

1.4 Forholdet til annen nasjonal veiledning 5

1.5 Forholdet til EUs strategier 5

1.5.1 Om EUs datastrategi 5

1.5.2 European Mobility Data Space (EMDS) 5

1.6 Dataveilederens utvikling og forvaltning 6

2 Behandling av personopplysninger 6

2.1 Innledning 6

2.2 Grunnprinsipper 6

2.3 Hva er en personopplysning 7

2.4 Behandling av personopplysninger 7

2.5 Behandlingsgrunnlag 8

2.6 Særlig om behandling til statistiske formål 9

3 Personvernroller 10

3.1 Ulike roller i personvernregelverket 10

3.2 Behandlingsansvarlig 10

3.3 Felles behandlingsansvar 11

3.3.1 Samhandling mellom behandlingsansvarlige 11

3.3.2 Når foreligger det et felles behandlingsansvar 11

3.3.3 Ansvaret til den enkelte felles behandlingsansvarlige 12

3.4 Databehandler 12

3.4.1 Hvem er databehandler 12

3.4.2 Databehandlers ansvar 12

3.5 Særlig om underdatabehandlere 13

4 Den registrertes rettigheter 13

4.1 Generelt 13

4.2 Særlig om mindreåriges rettigheter 14

4.3 Særlig om elektronisk billettering og anonyme alternativer 14

5 Anbefalinger om rutiner for informasjonssikkerhet og personvern 15

5.1 Innledning 15

5.2 Interne roller og ansvar i virksomheten 15
5.3 Ledelsens gjennomgang 16
5.4 Personvernombud 16
5.5 Medarbeidere, kompetanse og holdningsskapende arbeid 16
5.6 Behandlingsprotokoll 16
5.7 Vurdering av personvernkonsekvenser 17
5.8 Innebygd personvern 17
5.9 Valg av databehandlere 18
5.10 Håndtering av brudd på personopplysningssikkerheten 18
5.10.1 Brudd som ikke er meldepliktige til Datatilsynet 18
5.10.2 Meldingspliktige brudd 18
5.10.3 Underretting til den registrerte 19
5.11 Risikovurderinger av KI-løsninger 19
5.12 Særlig om IoT, sensorer, billetteringsteknologi 19
6 Deling og datasamarbeid 20
6.1 Innledning 20
6.2 Klassifisering av data 20
6.2.1 Minimumsbeskrivelse av datasettet 20
6.2.2 Klassifisering 20
6.2.3 Klassifisering ved behandling av personopplysninger 21
6.2.4 Om datasettet er underlagt andre begrensninger 21
6.2.5 Klassifiseringskonklusjon (resultat) 21
6.3 Vurdering av data som er eller inneholder personopplysninger 21
6.3.1 Overordnet 21
6.3.2 Forholdet til opprinnelig innsamling og behandlingsgrunnlag 22
6.3.3 Innsamlingsmåte (direkte/indirekte) og håndtering av informasjonsplikt 22
6.3.4 Viderebruk og forenlighet 23
6.3.5 Rollevurdering ved deling av personopplysninger 23
6.3.6 Særlig om utlevering av personopplysninger til statistikkformål hos mottaker 24
6.3.7 Systemer, dataflyt og behov for risikovurdering/DPIA 24
6.4 Tiltak ved deling av personopplysninger 24
6.5 Håndtering av taushetsbelagte og konfidensielle opplysninger 25
6.5.1 Overordnet 25
6.5.2 Lovbestemt taushetsplikt 26
6.5.3 Særlig om offentlige virksomheters forhold til forvaltningsloven 27
6.5.4 Anbefalt dokumentasjon ved deling av taushetsbelagte opplysninger 27
6.5.5 Forretningshemmeligheter etter forretningshemmelighetsloven 27
6.6 Håndtering av data underlagt andre rettigheter 28
6.6.1 Opphavsrett og databaserett 28
6.6.2 Lisenser, avtaler og tredjepartsrettigheter 28
6.6.3 Konsekvens ved manglende rettighetsavklaring 28
6.7 Sikre notoritet 28

7 Oversikt over gjeldende temaark og maler 29
7.1 Innledning 29
7.2 Temaark 29
7.3 Maler 29

0. Veilederens utforming

Veilederen er delt inn i to deler:

Del I: Hoveddokument
Hoveddokumentet (dette dokumentet) er Dataveilederens generelle del og gir oversikt over de mest sentrale krav og plikter som gjelder for aktørene. I hoveddokumentet redegjøres det for hvilke krav regelverket stiller til aktørene i bransjen, herunder beskrivelser av relevante vurderinger og aktiviteter den enkelte aktør må gjennomføre for å sikre etterlevelse.

Del II: Vedlegg
Det er utarbeidet følgende vedlegg til Dataveilederen:

Temaark
I disse dokumentene finnes oversikt over hvordan regelverket bør håndteres i praksis, i tillegg til eksempler på hvordan regelverket kan praktiseres for å være i overensstemmelse med krav til personvern og informasjonssikkerhet.

Maler
Det er etablert malverk for ulike vurderinger og aktiviteter som aktørene er pålagt å gjennomføre. Formålet med malene er å gi aktørene praktiske hjelpemidler i utføringen av disse. Malene skal sikre en systematisk, konsistent og lovmessig overholdelse av personvernkrav. Malene er vedlegg til hoveddokumentet.

1 Om veilederen

1.1 Bakgrunn og formål

Samferdselssektoren omfatter et bredt spekter av aktører, fra statlige, fylkeskommunale og kommunale myndigheter til offentlig og privateide transportforetak og leverandører av digitale tjenester.

Det foregår omfattende informasjonsutveksling mellom reisende, transportoperatører og forvaltere av infrastruktur på veg, bane, luft og sjø. Gjennom drift og bruk av transport- og infrastrukturtjenester behandles store mengder data, og en betydelig del av disse er personopplysninger. Dette inkluderer blant annet reise- og billetteringsinformasjon, posisjonsdata, trafikk- og hendelsesdata samt kommunikasjon mellom brukere, tjenesteleverandører og myndigheter.

Formålet med veilederen er å gi sektoren et felles, praktisk grunnlag for deling av data, særlig personopplysninger, på tvers av virksomheter. Veilederen pålegger ikke deling av data og er ikke rettslig bindende.

Veilederen gir råd om hvordan aktørene kan legge til rette for bedre utnyttelse av data som allerede samles inn, særlig med tanke på deling med andre aktører. Slik bruk av data forutsetter at virksomhetene har etablerte rammer for egen databehandling og oversikt over gjeldende regelverk. Veilederen inneholder:

- felles begreper, prinsipper og metoder for klassifisering, viderebruk og deling av data som er eller kan være personopplysninger
- praktiske fremgangsmåter for å vurdere delingssituasjoner, herunder behandlingsgrunnlag, forenlighet, rolleavklaringer og risikovurderinger
- tilgrensende rettslige rammer som ofte påvirker deling, herunder taushetsplikt, forretningshemmeligheter, rettighetsbegrensninger og relevant sektor- og EU-regelverk

Veilederen bygger på en forutsetning om at virksomhetene har et grunnleggende styringssystem for personvern og informasjonssikkerhet, uten å stille konkrete krav til hvordan dette skal være utformet. Samtidig inneholder veilederen sjekklister, anbefalte fremgangsmåter og eksempler som kan støtte virksomhetene i dette arbeidet.

Veilederen tar i begrenset grad for seg opprinnelig innsamling av data, herunder personopplysninger og bruk til etablerte formål. Den er heller ikke en uttømmende oversikt over alle regler som kan være relevante. Veilederen peker likevel på grunnleggende personvernkrav og typiske problemstillinger som ofte oppstår ved viderebruk og deling, og viser til temaark og maler for nærmere veiledning.

Veilederen er utformet for å være praktisk anvendbar for fagpersoner både med og uten juridisk bakgrunn, og skal bidra til felles forståelse og praksis på tvers av sektoren.

En oversikt over annet relevant regelverk som er hensyntatt i veiledningen, fremgår av punkt 1.3 og 1.5 nedenfor.

1.2 Verdien av å dele data

Deling av data mellom virksomheter er et sentralt virkemiddel for bedre samhandling, effektiv ressursbruk og utvikling av nye og forbedrede tjenester. En del av dataene som deles er personopplysninger, men også øvrige data kan ha stor samfunnsmessig og økonomisk verdi når de viderebrukes på en strukturert og ansvarlig måte.

Digitaliserings- og forvaltningsdepartementet publiserte i september 2024 Nasjonal digitaliseringsstrategi 2024–2030, som setter retningen for det digitale Norge. Strategien har et høyt ambisjonsnivå, med et overordnet mål om at Norge skal bli verdens mest digitaliserte land innen 2030. Bedre utnyttelse og viderebruk av data på tvers av virksomheter og sektorer er et sentralt virkemiddel for å nå dette målet.

Som ledd i dette arbeidet har Digitaliserings- og forvaltningsdepartementet mottatt NOU 2024:14 *Med lov skal data deles*, hvor det foreslås en ny datadelingslov og en ny dataforvaltningslov. Forslaget tar sikte på å etablere klarere og mer forutsigbare rammer for hvordan offentlige virksomheter kan gjøre data tilgjengelig for viderebruk på en måte som skaper verdi for andre. Utredningen legger til grunn gjennomføring av tre sentrale felleseuropeiske rettsakter: åpne data-direktivet (EU) 2019/1024, gjennomføringsforordningen om datasett med høy verdi (EU) 2023/138 og dataforvaltningsforordningen (EU) 2022/868.

Også Nasjonal transportplan 2025–2036 (NTP) fremhever betydningen av digitalisering og teknologiske muligheter i samferdselssektoren. I kapittel 9 pekes det på at effektiv bruk av data og ny teknologi kan bidra til en enklere reisehverdag, økt konkurranseevne og bedre ressursutnyttelse, samtidig som det støtter opp under nullvisjonen for drepte og hardt skadde. Transportsektoren forventes å bli stadig mer datadrevet, blant annet gjennom økt bruk av kunstig intelligens (KI), noe som forutsetter god dataforvaltning og tilgang til relevante og pålitelige datasett.

For å oppnå et mer samordnet transporttilbud understrekes behovet for videreutvikling av digitale verktøy for planlegging, bestilling og gjennomføring av reiser, herunder deling og standardisering av mobilitetsdata. En mer digitalisert og datadrevet samferdselssektor bidrar til å styrke transportsystemenes funksjon og gir grunnlag for mer effektiv utnyttelse av både infrastruktur og transporttilbud. Å realisere dette potensialet forutsetter en helhetlig tilnærming, der myndigheter, næringsliv og forskningsmiljøer samarbeider tett.

1.3 Forholdet til nasjonal lovgivning og sektorlovgivningen

Samferdselssektoren er regulert av omfattende sektorlovgivning som kan ha betydning for behandling, viderebruk og deling av data. Sektorlovgivningen gir rammer for hvilke data som kan behandles, og stiller i flere tilfeller særskilte krav eller begrensninger knyttet til utlevering, tilgjengeliggjøring eller viderebruk av opplysninger.

Eksempler på relevant sektorlovgivning er yrkestransportlova, jernbaneloven, veglova, vegtrafikkloven, luftfartsloven, havne- og farvannsloven, ITS-loven, samt tilhørende forskrifter. Også sektorvise regler om trafikkstyring, beredskap, sikkerhet og tilsyn kan inneholde bestemmelser som påvirker adgangen til å dele eller viderebruke data.

Det er utarbeidet et eget temaark om sentral sektorlovgivning, som gir en samlet oversikt over relevante lover og forskrifter i samferdselssektoren. Sektorlovgivningens betydning for viderebruk og deling av data er også omtalt i flere av de øvrige temaarkene, der regelverket er relevant i konkrete delingssituasjoner. Se temaark T02 – Oversikt over lover.

I tillegg til sektorlovgivning som direkte regulerer datadeling, vil det ofte være nødvendig å vurdere regelverk om taushetsplikt og vern av forretningshemmeligheter. Dette omfatter blant annet lov om forretningshemmeligheter for private virksomheter og lovbestemt taushetsplikt etter forvaltningsloven for forvaltningsorganer.

1.4 Forholdet til annen nasjonal veiledning

Dataveilederen gir anbefalinger om hvordan krav til personvern og personopplysningssikkerhet kan håndteres i samferdselssektoren. Veilederen bygger på gjeldende regelverk og utfyller generell veiledning fra blant annet Datatilsynet og Digitaliseringsdirektoratet, uten å etablere nye rettslige plikter.

På enkelte områder finnes det sektorspesifikke normerende dokumenter som gir mer detaljerte føringer. Der slike dokumenter foreligger, bør de legges til grunn i det konkrete arbeidet. Dataveilederen gir i disse tilfellene overordnede anbefalinger og vurderingsmomenter knyttet til personvern og personopplysningssikkerhet.

Håndbok V821 del 5 om elektronisk billettering er det sentrale normerende dokumentet for billetteringsløsninger i kollektivtransporten. Håndboken gir konkrete føringer for utforming og drift av løsninger, herunder forhold som også har direkte betydning for behandling av personopplysninger.

De personvernrettslige grunnprinsippene som ligger til grunn for Dataveilederen er ment å forstås og anvendes i samsvar med håndbok V821 del 5. På det konkrete området elektronisk billettering bør virksomheter primært se hen til håndbok V821 del 5 ved utforming, anskaffelse og drift av løsninger. Dataveilederen kommer i tillegg og gir supplerende anbefalinger for vurderinger av behandlingsgrunnlag, rolleavklaringer, risikovurderinger og eventuell deling og viderebruk av billetteringsdata.

1.5 Forholdet til EUs strategier

1.5.1 Om EUs datastrategi

EUs datastrategi (European Strategy for Data) er den overordnede politiske rammen for utviklingen av et felles europeisk marked for data. Strategien har som mål å styrke Europas konkurranseevne, teknologiske suverenitet og evne til å utvikle data-drevne tjenester, samtidig som individers og virksomheters rettigheter ivaretas.

Kjernen i datastrategien er etableringen av Common European Data Spaces på tvers av sektorer, som skal gjøre mer data tilgjengelig for bruk til forskning, innovasjon, offentlig tjenesteutvikling og næringsutvikling, under tydelige krav til kontroll, tillit og sikkerhet.

Strategien er fulgt opp gjennom sentrale rettsakter som Data Governance Act (DGA), Data Act, Åpne data-direktivet og HVD-forordningen, som samlet skal sikre trygg deling, viderebruk og tilgang til data i EU/EØS.

1.5.2 European Mobility Data Space (EMDS)

EMDS er et av de sektorielle dataspace-initiativene under EUs datastrategi. Formålet er å legge til rette for trygg, effektiv og interoperabel deling av mobilitets- og transportdata på tvers av offentlige og private aktører i Europa. EMDS skal støtte overgangen til et mer bærekraftig, smart og integrert transportsystem, i tråd med både Sustainable and Smart Mobility Strategy (SSMS) og European Green Deal.

EMDS skal ikke være én felles EU-database, men et rammeverk for å koble sammen eksisterende og nye datadomener gjennom felles prinsipper, styringsmodeller og tekniske byggeklosser. Kommisjonens EMDS-kommunikasjon fra november 2023 fastslår at arbeidet vil bygge videre på relevante EU-regelverk, særlig Data Governance Act (DGA), Data Act, ITS-direktivet og datadelingstiltak utviklet gjennom ekspertfora som Digital Transport and Logistics Forum (DTLF).

Kjernen i EMDS er et såkalt interlinking layer, et «koblingslag». Dette laget gjør ulike datasett og dataspace-miljøer søkbare, tilgjengelige og interoperable på tvers av transportformer og medlemsland. EMDS er ment å bidra til bedre datatilgang og legge til rette for både sanntidsdata, standardiserte grensesnitt og bedre gjenfinning av datasett på tvers av Europa.

Gevinster forventes for både reisende, myndigheter og næringsliv: mer effektiv trafikkstyring, bedre multimodal reiseinformasjon, økt sikkerhet, enklere grensekryssende transport og nye tjeneste- og innovasjonsmuligheter basert på tilgjengelige data. Særlig små og mellomstore virksomheter (SMB-er) fremheves som potensielle vinnere av enklere og mer rettferdig tilgang til mobilitetsdata.

Utviklingen av EMDS er et gradvis og iterativt arbeid, og vil kreve tett medvirkning fra mobilitets- og transportsektoren i alle medlemsstater og EØS-land. Norske aktører innen mobilitet, kollektivtransport, trafikkdata, infrastruktur og billettering bør følge arbeidet nøye, da EMDS forventes å påvirke hvordan data deles og gjenbrukes på tvers av sektoren i årene fremover.

1.6 Dataveilederens utvikling og forvaltning

Veilederen er utarbeidet av deltakere i det tverrsektorielle datasamarbeidet ved Jernbanedirektoratet, Statens vegvesen, Avinor AS, Nye Veier AS, Entur AS, Bane Nor SF. I tillegg har Innlandet fylkeskommune, Ruter AS, Vygruppen og Go Ahead bidratt i utarbeidelsen.

Veilederen forvaltes av en Rådgivende gruppe for Dataveilederen. Rådgivende gruppes overordnede mål for veilederen er å gi råd om hvordan veilederen skal utvikles for å være oppdatert og i samsvar med til enhver tid gjeldende regelverk.

Entur AS er sekretariat for Dataveilederen. Det er utarbeidet mandat til Rådgivende gruppe for Dataveilederen og instruks for sekretariatets arbeid.

2 Behandling av personopplysninger

2.1 Innledning

Dette kapittelet gir et overordnet rettslig utgangspunkt for behandling av personopplysninger i samferdselssektoren. Formålet er å etablere en felles forståelse av de grunnleggende begrepene og rammene i personvernregelverket, som danner grunnlag for veilederens videre omtale av viderebruk og deling av data.

Kapittelet redegjør for hva som regnes som personopplysninger, hva som menes med «behandling», og hvilke grunnprinsipper som gjelder for all behandling av personopplysninger. Videre beskrives kravene til behandlingsgrunnlag, herunder når samtykke, avtale, rettslig forpliktelse, allmennhetens interesse og berettigede interesser kan benyttes. Det gis også en særskilt omtale av behandling til statistiske formål, som er særlig relevant i samferdselssektoren.

Kapittelet gir ikke en fullstendig fremstilling av alle rettslige krav etter personvernregelverket. Der temaene behandles nærmere i egne temaark eller maler, vises det til disse.

2.2 Grunnprinsipper

Grunnprinsippene i personvernregelverket gjelder for samferdselssektoren på samme måte som i andre sektorer.

Grunnprinsippene for behandling av personopplysninger følger av personvernforordningen artikkel 5.

Grunnprinsippene innebærer at personopplysninger skal behandles i samsvar med kravene til:

- lovlighet, rettferdighet og åpenhet,
- formålsbegrensning,
- dataminimering,
- riktighet,
- lagringsbegrensning,
- integritet og konfidensialitet, samt
- ansvarlighet

Grunnprinsippene utgjør det overordnede rettslige rammeverket for all behandling av personopplysninger. Ved vurderinger av viderebruk og deling av data vil særlig prinsippene om formålsbegrensning, dataminimering, lagringsbegrensning og integritet og konfidensialitet være sentrale.

Nærmere veiledning om hvordan grunnprinsippene kan anvendes i praksis ved viderebruk og deling av data, fremgår av egne temaark.

2.3 Hva er en personopplysning

Begrepet personopplysninger er definert i personvernforordningen artikkel 4 nr. 1, og lyder som følger:

> *«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*

Det foregår viktig rettsutvikling på dette området i EU, som innebærer at grensene for hva som regnes som en personopplysning er relativt til hva den enkelte virksomhet kan identifisere. Virksomhetene bør derfor være klar over at grensen mellom hva som er en personopplysning og ikke, kan være vanskelig å trekke.

Identifiserbarhet vurderes relativt

Om opplysninger er personopplysninger, beror ikke bare på om navn eller direkte identifikatorer forekommer, men på om en person kan identifiseres i praksis – direkte eller indirekte. Vurderingen bør ta utgangspunkt i avsenders og mottakers faktiske muligheter for identifisering, herunder tilgang til andre datasett, sammenstillingsmuligheter og teknisk kompetanse.

I samferdselssektoren vil særlig posisjons- og bevegelsesdata over tid, kombinasjoner av tid og sted, samt bruk av unike enhets- eller kundeidentifikatorer ofte innebære at data er personopplysninger, selv om de fremstår som «avidentifiserte».

Virksomheten bør dokumentere identifiserbarhetsvurderingen som del av klassifisering og risikovurdering.

Henvisning: Temaark T03 - Hva er en personopplysning

2.4 Behandling av personopplysninger

Begrepet behandling av personopplysninger følger av personvernforordningen artikkel 4 nr. 2, og lyder som følger:

> *«behandling» enhver operasjon eller rekke av operasjoner som gjøres med personopplysninger, enten automatisert eller ikke, f.eks. innsamling, registrering, organisering, strukturering, lagring, tilpasning eller endring, gjenfinning, konsultering, bruk, utlevering ved overføring, spredning eller alle andre former for tilgjengeliggjøring, sammenstilling eller samkjøring, begrensning, sletting eller tilintetgjøring.*

Det skal svært lite til før en behandlingsaktivitet er omfattet av definisjonen, hvilket betyr at tilnærmet enhver befatning som virksomheter har med personopplysninger, vil regnes som behandling. Det praktiske vurderingstemaet er derfor normalt om opplysningene i det hele tatt er personopplysninger, jf. punkt 2.3.

Virksomhetene bør være oppmerksomme på at personopplysningsloven § 2 bruker begrepet «automatisert» behandling, hvilket er et begrep som kan misforstås. Begrepet skal forstås slik at det favner all behandling ved bruk av informasjonsteknologi, ikke at prosessen må være «selvgående». Loven bruker for øvrig formuleringen «helt eller delvis automatisert» – dvs. at det er tilstrekkelig at behandlingen delvis foretas ved hjelp av informasjonsteknologi.

Når det gjelder spørsmålet om hva som er en enkelt behandling, og hva som regnes som «en rekke av operasjoner», bør det sees hen til hvorvidt behandlingsansvarlig utfører flere operasjoner for det samme formålet. I så fall bør virksomheten se disse samlet som én behandling. Dette formålsbaserte skillet har røtter tilbake til personopplysningsloven av 2000.

2.5 Behandlingsgrunnlag

Utgangspunktet er at all behandling av personopplysninger er forbudt, med mindre man har et unntak i form av et behandlingsgrunnlag.

Behandling av personopplysninger krever et gyldig behandlingsgrunnlag. Før behandling starter, eller ved endringer i eksisterende behandling, skal behandlingsansvarlig sørge for at behandlingsgrunnlaget dekker den aktuelle behandlingen og de formålene personopplysningene brukes til. Dette gjelder alle former for behandling, herunder innsamling, lagring, viderebruk og utlevering.

Dersom personopplysninger viderebrukes til et annet formål enn det opprinnelige, må det vurderes om viderebruken er forenlig med det opprinnelige formålet, eller om det kreves et nytt behandlingsgrunnlag.

Personvernforordningen artikkel 6 nr. 1 oppstiller seks alternative behandlingsgrunnlag:

a) samtykke fra den registrerte
b) oppfyllelse av avtale med den registrerte
c) oppfyllelse av en rettslig forpliktelse
d) vern av vitale interesser
e) utførelse av en oppgave i allmennhetens interesse eller utøvelse av offentlig myndighet
f) ivaretakelse av en berettiget interesse

Ett behandlingsgrunnlag per behandling og formål

For hver behandling av personopplysninger og for hvert formål skal virksomheten fastsette ett behandlingsgrunnlag.

Det er ikke riktig å basere samme behandling for samme formål på flere behandlingsgrunnlag i parallell (for eksempel både samtykke og berettiget interesse). En slik tilnærming er uforenlig med personvernregelverkets system og skaper uklarhet om hvilke rettigheter som gjelder for de registrerte og hvilke plikter som påhviler virksomheten.

Dersom ulike deler av en løsning har ulike formål, må disse behandlingsaktivitetene skilles og vurderes hver for seg, med egne behandlingsgrunnlag der dette er relevant.

Offentlige virksomheter

For offentlige virksomheter i samferdselssektoren vil behandlingsgrunnlag etter artikkel 6 nr. 1 bokstav c) (rettslig forpliktelse) og e) (oppgave i allmennhetens interesse eller offentlig myndighetsutøvelse) ofte være mest aktuelle. Dette gjelder særlig behandling knyttet til planlegging, drift, styring, statistikk, tilsyn og rapportering innen transport- og mobilitetsområdet. Her kreves det nærmere behandlingsgrunnlag i lov eller forskrift.

Bruk av samtykke som behandlingsgrunnlag bør vurderes med varsomhet i offentlige virksomheter, særlig der det foreligger et avhengighetsforhold mellom den registrerte og virksomheten.

Private virksomheter

For private virksomheter (kommersielle som ikke-kommersielle) vil behandlingsgrunnlag etter artikkel 6 nr 1 bokstav a) (samtykke fra den registrerte), b) (oppfyllelse av avtale) og f) (berettiget interesse) ofte være de mest

sentrale, særlig ved behandling av personopplysninger knyttet til levering av transporttjenester, billettering, kundehåndtering og tjenesteutvikling.

Ved bruk av berettiget interesse må virksomheten foreta en konkret interesseavveiing, der hensynet til virksomhetens formål veies mot den registrertes personvern.

Dersom flere behandlingsgrunnlag kan være aktuelle, skal virksomheten fastsette ett behandlingsgrunnlag per formål, og dette bør dokumenteres som del av virksomhetens personvernstyring.

2.6 Særlig om behandling til statistiske formål

Behandling av personopplysninger til statistiske formål er særlig relevant i samferdselssektoren, blant annet i forbindelse med analyse, planlegging, styring, forskning og rapportering. I den utstrekning statistiske datasett ikke er anonyme, gjelder personvernregelverket fullt ut.

Viderebehandling av personopplysninger til statistiske formål anses ikke som uforenlig med de opprinnelige formålene, jf. personvernforordningen artikkel 5 nr. 1 bokstav b, forutsatt at behandlingen skjer i samsvar med artikkel 89. Det skal derfor ikke foretas en forenlighetsvurdering etter artikkel 6 nr. 4 ved slik viderebehandling.

Behandling til statistiske formål krever likevel et gyldig behandlingsgrunnlag etter personvernforordningen artikkel 6 nr. 1. De følgende behandlingsgrunnlag er særlig aktuelle:

- artikkel 6 nr. 1 bokstav e (oppgave i allmennhetens interesse), jf. personopplysningsloven § 8,
- artikkel 6 nr. 1 bokstav c (rettslig forpliktelse), der statistikkproduksjon følger av lov eller forskrift, eller
- artikkel 6 nr. 1 bokstav f (berettiget interesse), særlig for private aktører, forutsatt at interesseavveiningen faller ut i virksomhetens favør.

Dersom behandlingen skjer med grunnlag i bokstav c eller e, kreves det et supplerende rettsgrunnlag i nasjonal rett i samsvar med artikkel 6 nr. 3. Hvor detaljert dette rettsgrunnlaget må være, beror på behandlingens karakter og hvor inngripende den er.

Personvernforordningen artikkel 89 stiller særskilte krav til behandling til statistiske formål. Det følger blant annet at:

- det ikke skal behandles flere personopplysninger enn nødvendig for formålet (dataminimering),
- detaljnivået i dataene skal begrenses der dette er mulig,
- det skal gjennomføres egnede tekniske og organisatoriske tiltak for å sikre de registrertes rettigheter og friheter.

Reglene om de registrertes rettigheter og om lagring og sletting gjelder som utgangspunkt også ved behandling til statistiske formål, med de særskilte tilpasninger som følger av regelverket.

Statistikk innebærer ikke nødvendigvis anonymisering

Behandling av personopplysninger til statistiske formål innebærer ikke i seg selv at opplysningene er anonymisert eller faller utenfor personvernregelverket.

Viderebehandling til statistiske formål anses som forenlig viderebruk, jf. personvernforordningen artikkel 5 nr. 1 bokstav b, men forutsetter at behandlingen skjer i samsvar med artikkel 89 og at det foreligger gyldig behandlingsgrunnlag. Det vil si at anonymisering er hovedregelen dersom formålet med viderebehandling til statistikk kan oppfylles på den måten. Hvis ikke kan pseudonymisering være aktuelt.

Statistiske datasett vil ofte være pseudonymiserte eller aggregert, men kan fortsatt være personopplysninger dersom enkeltpersoner kan identifiseres direkte eller indirekte. Kravene til dataminimering, lagringsbegrensning og egnede tekniske og organisatoriske tiltak gjelder derfor fullt ut.

Henvisning: Temaark T05 - Behandling til statistiske formål

3 Personvernroller

3.1 Ulike roller i personvernregelverket

Innenfor personvernregelverket finnes det to sentrale roller: behandlingsansvarlig og databehandler. Rollene er definert i GDPR artikkel 4 nr. 7 og 8. Formålet med de ulike rollene er å plassere ansvar for behandling av personopplysninger. Behandlingsansvarlig har det overordnende ansvaret for personopplysningene, og bestemmer både formålet de skal behandles for og hvilke virkemidler som skal brukes. Databehandler behandler personopplysninger *på vegne* av behandlingsansvarlig. Mer om dette nedenfor.

3.2 Behandlingsansvarlig

Det kan være flere behandlingsansvarlige for samme behandlingsaktivitet. De kan enten være ansvarlige alene for hver sin del av behandlingsaktiviteten, eller ha et felles behandlingsansvar.

Definisjonen av en behandlingsansvarlig følger av GDPR artikkel 4 nr. 7 og består av to deler. For det første er virksomheten behandlingsansvarlig dersom den alene eller sammen med en annen «bestemmer formålet med behandlingen av personopplysninger og hvilke midler som skal benyttes». Når formål og midler er fastsatt i nasjonal rett, kan det samtidig være angitt i lov eller forskrift at det er en bestemt virksomhet som er behandlingsansvarlig.[1]

Behandlingsansvarlig skal:

- definere formålet med behandlingen
- delegere myndighet og oppgaver
- etablere og etterleve styringssystemet
- gjennomføre risikovurderinger og personvernkonsekvensvurderinger der det er nødvendig
- sikre den registrertes rettigheter
- etablere og dokumentere tekniske og organisatoriske tiltak
- inngå og følge opp avtaler
- håndtere avvik

I tillegg er behandlingsansvarlig den parten som i hovedsak kan ansvarliggjøres, det vil si motta pålegg fra tilsynsmyndigheter, ilegges overtredelsesgebyr (bøter) og bli erstatningsansvarlig dersom regelverket ikke overholdes.

Behandlingsansvarlig er ansvarlig for å opptre i henhold til personvernprinsippene. Dette innebærer at personopplysninger skal:

- behandles på en lovlig måte (gyldig behandlingsgrunnlag)

[1] Se i den forbindelse også EDPB Guidelines 07/2020 on the concept of controller.

- behandles på en rettferdig måte (med respekt for de registrertes interesser og rettigheter)
- behandles på en åpen måte (oversiktlig, forutsigbar og forståelig informasjon) med hensyn til den registrerte (brukeren)
- bare registreres for bestemte formål som skal være legitime
- være tilgjengelig - bare benyttes til de formål de er registrert for, med mindre det finnes behandlingsgrunnlag for andre formål
- være relevante, adekvate, korrekte og om nødvendig oppdaterte for de formål de er registrert for
- lagres slik at det ikke er mulig å identifisere de registrerte i lengre perioder enn det som er nødvendig for formålene
- sikres mot uautorisert tilgang, endring, ødeleggelse og spredning

Behandlingsansvarlig skal dokumentere at virksomheten har gjennomført tiltak for å etterleve personvernforordningen.

3.3 Felles behandlingsansvar

3.3.1 Samhandling mellom behandlingsansvarlige

I samferdselssektoren er det vanlig at ulike aktører, som kollektivtransportselskaper, vegmyndigheter, flyselskaper og IT-leverandører, opererer som selvstendige behandlingsansvarlige. Dette betyr at hver enkelt aktør er ansvarlig for hvordan de behandler personopplysninger innenfor sin virksomhet. På mange områder i sektoren skjer det nødvendigvis en stor grad av samhandling gjennom bruk av felles systemer eller viderebruk av ulike typer opplysninger. Det er avgjørende å sikre at hver aktør har oversikt over rammene for sitt ansvar, herunder hvem som er behandlingsansvarlig og hvem som er databehandler for ulike behandlingsaktiviteter. I mange tilfeller må det også avklares hvorvidt man står overfor et felles behandlingsansvar.

3.3.2 Når foreligger det et felles behandlingsansvar

Felles behandlingsansvar foreligger dersom to eller flere virksomheter i *fellesskap* bestemmer formålet med en behandling og hvilke midler som skal benyttes. Det må gjøres en selvstendig vurdering i det enkelte tilfellet om partene i fellesskap avgjør formål og midler med behandlingen.

Retningslinjene fra European Data Protection Board (EDPB Guidelines 07/2020 on the concepts of controller and processor) presiserer at felles behandlingsansvar kan foreligge selv om partene ikke har like stor innflytelse, og selv om ansvaret gjelder ulike faser av behandlingen. Det er tilstrekkelig at partene i fellesskap påvirker formål og/eller vesentlige midler på en måte som gjør at behandlingen ikke ville funnet sted i samme form uten deres samlede beslutninger.

Dette aktualiseres særlig i samferdselssektoren, blant annet fordi det finnes flere tilfeller der løsninger der én aktør forestår innsamling og strukturering av data før videre utlevering til andre virksomheter. I denne sammenheng kan det vises til følgende samarbeidsformer og løsninger:

- sømløse mobilitetskjeder på tvers av virksomheter
- felles billetteringsløsninger
- integrerte reiseplanleggingsplattformer
- offentlig-privat samarbeid
- offentlig-offentlig samarbeid

For offentlige aktører er det viktig å være oppmerksom på at det forhold at en behandling gjelder en offentlig oppgave på et lovregulert område, ikke i seg selv alltid avgjør om det foreligger felles

behandlingsansvar. Lovgivningen regulerer ofte *oppgaven* eller det materielle ansvaret, men fastsetter ikke nødvendigvis hvordan behandlingsansvaret etter personvernforordningen skal fordeles mellom flere involverte virksomheter. Selv der behandlingen skjer som ledd i offentlig myndighetsutøvelse eller allmennhetens interesse, må det derfor ofte foretas en selvstendig vurdering av hvordan ansvaret er fordelt.

Vurdering av om det foreligger felles behandlingsansvar

Felles behandlingsansvar foreligger bare der to eller flere virksomheter i fellesskap fastsetter både formålet med behandlingen og de sentrale midlene.

At flere aktører er involvert i samme system, datasamarbeid eller verdikjede, innebærer ikke i seg selv et felles behandlingsansvar. I samferdselssektoren vil aktører ofte behandle samme type data, men til ulike formål og innenfor egne ansvarsområder. Dette tilsier normalt selvstendig behandlingsansvar, ikke felles behandlingsansvar.

Dersom to eller flere virksomheter anses å være felles behandlingsansvarlige, skal det etableres en skriftlig ordning i samsvar med personvernforordningen artikkel 26, som fastsetter partenes respektive ansvar for å oppfylle forpliktelsene etter forordningen.

3.3.3 Ansvaret til den enkelte felles behandlingsansvarlige

Når det foreligger felles behandlingsansvar, må aktørene ha et bevisst forhold til rammene for deres respektive ansvar. Partene bør avtale hvordan ansvaret skal fordeles mellom dem. Det er i utgangspunktet full avtalefrihet, både når det gjelder form og struktur. Det bør imidlertid inngås en skriftlig avtale, slik at det er tydelig hvem som har ansvar for hva. Avtalen må som helhet dekke kravene i forordningen. Det er viktig å understreke at selv om ansvarsfordelingen mellom partene kan avtales innenfor rammen av GDPR, vil begge virksomheter i fellesskap være ansvarlige for etterlevelse av regelverket. Dette innebærer at den registrerte skal kunne henvende seg til samtlige behandlingsansvarlige virksomheter.

Alle felles behandlingsansvarlige må kunne demonstrere hvilke vurderinger som er gjort i forbindelse med behandlingsansvaret. Dette gjelder for både beslutningen om at det foreligger felles behandlingsansvar, og hvordan ansvarsfordelingen er fastlagt mellom partene. Prinsippet om åpenhet gjelder likefullt ved felles behandlingsansvar som ellers, og innebærer at hver behandlingsansvarlig må være åpen om hvordan personopplysninger behandles. Dersom man ikke har gitt informasjon om dette kan behandlingen være ulovlig, og bøter kan ilegges.

3.4 Databehandler

3.4.1 Hvem er databehandler

En databehandler er en virksomhet som behandler personopplysninger på vegne av den behandlingsansvarlige, jf. personvernforordningen artikkel 4 nr. 8. Bruk av databehandler forutsetter at den behandlingsansvarlige bare benytter databehandlere som gir tilstrekkelige garantier for at behandlingen skjer i samsvar med personvernregelverket, jf. artikkel 28 nr. 1.

Databehandler kan som hovedregel kun behandle personopplysninger på vegne av den behandlingsansvarlige, og ikke til egne formål som f.eks. markedsføring, analyser eller trening av KI. Dersom man bruker en databehandler, skal man inngå en databehandleravtale.

3.4.2 Databehandlers ansvar

Databehandlerens plikter følger særlig av GDPR artikkel 28 og skal fastsettes i en skriftlig databehandleravtale eller annet rettslig dokument. Avtalen skal blant annet angi formålet med behandlingen, behandlingens varighet og art, hvilke personopplysninger som behandles, og partenes rettigheter og plikter.

Databehandler skal blant annet:

- behandle personopplysninger utelukkende etter dokumenterte instrukser fra den behandlingsansvarlige, jf. artikkel 28 nr. 3 bokstav a,
- sikre at personer som behandler personopplysninger er underlagt taushetsplikt, jf. artikkel 28 nr. 3 bokstav b,
- gjennomføre egnede tekniske og organisatoriske tiltak for å sikre et tilstrekkelig sikkerhetsnivå, jf. artikkel 28 nr. 3 bokstav c og artikkel 32,
- ikke engasjere underdatabehandler uten forutgående særskilt eller generell skriftlig godkjenning fra den behandlingsansvarlige, jf. artikkel 28 nr. 2,
- sørge for at eventuelle underdatabehandlere pålegges tilsvarende personvernforpliktelser, og være ansvarlig overfor den behandlingsansvarlige dersom disse ikke oppfylles, jf. artikkel 28 nr. 4,
- bistå den behandlingsansvarlige med å oppfylle plikter etter personvernregelverket, herunder knyttet til de registrertes rettigheter, informasjonssikkerhet, avvikshåndtering og personvernkonsekvensvurderinger, jf. artikkel 28 nr. 3 bokstav e og f,
- slette eller tilbakelevere personopplysninger ved avslutning av tjenesten, med mindre videre lagring følger av lov, jf. artikkel 28 nr. 3 bokstav g,
- gjøre tilgjengelig nødvendig informasjon for å dokumentere etterlevelse og muliggjøre revisjon, jf. artikkel 28 nr. 3 bokstav h.

Databehandler kan ikke ha egne formål

En databehandler behandler personopplysninger på vegne av den behandlingsansvarlige og kan i den forbindelse ikke behandle opplysningene til egne formål.

Dersom en aktør fastsetter egne formål med behandlingen, eller bruker opplysningene til analyser, produktutvikling, gjenbruk eller andre selvstendige formål, vil aktøren som hovedregel være selvstendig behandlingsansvarlig for denne behandlingen, jf. GDPR artikkel 28 nr. 10.

Teknisk frihet, metodevalg eller bruk av standardløsninger innebærer ikke i seg selv behandlingsansvar, så lenge formål og sentrale midler er fastsatt av den behandlingsansvarlige.

3.5 Særlig om underdatabehandlere

Når databehandler benytter seg av underdatabehandler er databehandleren ansvarlig for at underleverandøren oppfyller sine forpliktelser. Dette innebærer at underdatabehandler har et selvstendig ansvar for å opprettholde informasjonssikkerhet og personvernet til de registrerte. Dette skal ivaretas gjennom skriftlig avtale mellom databehandler og underdatabehandler.

Avtalen mellom partene må fastsette at underdatabehandleren er underlagt de samme pliktene som databehandleren i henhold til databehandleravtalen. Avtalen skal kunne tilgjengeliggjøres for behandlingsansvarlig.

4 Den registrertes rettigheter

4.1 Generelt

Det er den registrerte som får vern etter GDPR og er den som personopplysninger dreier seg om. Den registrerte er alltid en levende, fysisk person, og kan ikke være f.eks. et selskap eller liknende selv om selskapsnavnet er det samme som et personnavn. Den registrerte får gjennom GDPR et sett med rettigheter som virksomhetene bør være kjent med.

For at en person skal få status som registrert må det være mulig å knytte personopplysninger til en bestemt person, altså må personopplysningene kunne identifisere personen.

Reglene om de registrertes rettigheter handler om hvilke rettigheter den enkelte bruker, reisende eller andre som er gjenstand for behandling besitter. Det er den behandlingsansvarlige som plikter å oppfylle disse rettighetene.

Plikten til å innfri den registrertes rettigheter har nær sammenheng med den behandlingsansvarliges internkontrollsystem. Internkontrollsystemet skal beskrive hvordan den behandlingsansvarlige skal forholde seg til rettighetene gjennom implementering av rutiner og aktiviteter, slik at den registrertes rettigheter blir overholdt.

For mer informasjon om hvilke rettigheter den registrerte har, og hvilke plikter som påhviler den behandlingsansvarlige i denne forbindelse, se temaark «T04 – registrertes rettigheter».

4.2 Særlig om mindreåriges rettigheter

Utgangspunktet er at vurderingen av mindreåriges kompetanse må ta hensyn til både personvernregelverket og alminnelige regler om barns handleevne og representasjon.

Hovedregelen er at den som er under 18 år er mindreårig og ikke har full rettslig handleevne (jf. vergemålsloven § 9 om rettslig handleevne). Før dette må foreldrene eller den med foreldreansvar samtykke på barnets vegne. Barn under 18 år kan i noen situasjoner likevel gi samtykke selv dersom de etter en konkret vurdering er i stand til å gi et informert og frivillig samtykke (jf. barneloven § 33 og de alminnelige kravene til gyldig samtykke), jf. også Datatilsynets nettsider om dette.[2] For samtykke til informasjonssamfunnstjenester gjelder likevel særregelen i personvernforordningen artikkel 8, jf. personopplysningsloven § 5.

Etter hvert som barnets selvråderett øker og foreldreansvaret minker, må det også kunne legges til grunn at den mindreårige får flere selvstendige rettigheter etter GDPR som kan håndheves på egne vegne.

Generelt sett har personer over 15 år kompetanse til å inngå avtaler med midler stilt til rådighet eller som de selv har tjent (vergemålsloven § 12). Dette gjelder også ved kjøp av transporttjenester og personen bør dermed også kunne samtykke til behandling av personopplysninger i den sammenhengen.

Et praktisk eksempel som kan komme opp knyttet til transport er ileggelse av kontrollgebyr for barn. For barn under 15 år er det ikke anledning til å ilegge kontrollgebyr. Siden mindreårige over 15 år har rett til å inngå visse «dagligdagse» avtaler, slik som kjøp av billett til kollektivtransport, vil de også akseptere de vilkår som følger med. Dersom vilkårene brytes, kan mindreårige i denne aldersgruppen ilegges et kontrollgebyr, og det er den mindreårige selv som er ansvarlig for å betale. Foreldrene er følgelig ikke uten videre økonomisk ansvarlige. Gebyret bør ikke regnes som en gjeldsstiftelse, men som en sanksjon basert

[2] Samtykke fra mindreårige

på en allerede inngått avtale. Dette skiller seg dermed fra tilfeller der foreldre er økonomisk ansvarlige, for eksempel ved skadeforvoldelse.

4.3 Særlig om elektronisk billettering og anonyme alternativer

Mulighet til å bevege seg fritt uten at reiser og passeringer systematisk registreres eller kan spores tilbake til den enkelte, kan utledes av vernet om privatliv etter Grunnloven § 102 og Den europeiske menneskerettskonvensjonen artikkel 8. I denne sammenheng omtales gjerne prinsippet om retten til anonym ferdsel. Prinsippet har særlig aktualitet i transportsektoren, der elektroniske betalings- og registreringssystemer gjør det mulig å følge bevegelsesmønstre over tid.

Det foreligger ulike oppfatninger i juridisk teori og praksis om hvorvidt enhver behandling av reise- og passeringsopplysninger innebærer et inngrep i retten til privatliv etter EMK artikkel 8, og det er mange ulike rettskilder som omtaler problemstillingen knyttet til spørsmålet uten at veilederen går i detaljer om dette. Spørsmålet må uansett vurderes konkret av den enkelte virksomhet, med utgangspunkt i behandlingens art, omfang, formål og kontekst. Det må i denne vurderingen særlig legges vekt på om behandlingen legger til rette for systematisk eller omfattende registrering av ferdsel, eller muliggjør kartlegging av bevegelsesmønstre over tid, ettersom slike forhold ofte vil kunne tilsi at det foreligger et inngrep. Offentlige aktører bør på denne bakgrunn sikre at behandling som åpner for slik registrering eller kartlegging, har et tilstrekkelig klart rettslig grunnlag i lov.

Det er for øvrig viktig å skille mellom anonym ferdsel (anonyme løsninger) og såkalte sporfrie løsninger. Med anonym ferdsel siktes det til at den reisende i praksis kan benytte transporttjenesten uten at reiser og passeringer systematisk registreres på en måte som kan knyttes tilbake til vedkommende. En anonym løsning er typisk en løsning der den reisende kan kjøpe og bruke et reiseprodukt uten å opprette konto, oppgi identitet eller ta i bruk en varig identifikator (for eksempel et personlig kundenummer), slik at det ikke bygges opp en identifiserbar reisehistorikk som standard.

Forskjellen kan illustreres med følgende eksempler:

1. Anonym ferdsel / anonym løsning kan være kjøp og bruk av en upersonlig billett eller et upersonlig reisemedium uten registrering, der kontroll kan gjennomføres ved å verifisere billettens gyldighet uten at reisen knyttes til en identitet eller brukerprofil.

2. Sporfri løsning kan være en løsning der billett, brikke eller app er knyttet til en bruker eller konto for å muliggjøre betaling og kontroll, men der reise- eller passeringsdetaljer automatisk slettes raskt, og der opplysninger som eventuelt beholdes over tid er sterkt begrenset i omfang og detaljeringsgrad.

5 Anbefalinger om rutiner for informasjonssikkerhet og personvern

5.1 Innledning

I dette kapittelet gis det anbefalinger og en oversikt over hvilke typer rutiner som bør inngå i virksomhetens styringssystem, herunder internkontrollsystem for personvern og informasjonssikkerhet.

Med styringssystem menes her formalisering av hvordan virksomheten planlegger, gjennomfører, evaluerer/kontrollerer og korrigerer etterlevelse av relevant regelverk, krav og avtaler.

Rutiner for informasjonssikkerhet og personvern bør inngå som en del av det totale styringssystemet (internkontrollen) i virksomheten. Dette gjelder særlig i vurderingen av egnet sikkerhetsorganisasjon, arbeidsoppgaver, kontrolloppgaver og tiltak innen informasjonssikkerhet (for eksempel tilgangsstyring, logging, fysisk sikring, beredskap mv.). Ved valg av egnede tekniske og organisatoriske tiltak skal virksomheten vurdere tiltakene opp mot virksomhetens art og omfang for behandling av personopplysninger.

Styringssystemet skal dokumenteres. Dokumenter angitt i styringssystemet skal holdes løpende oppdatert og arkiveres fra det tidspunktet dokumentet ble erstattet med en ny gjeldende versjon. Dette kan f.eks. være rutiner for sikkerhetsrevisjoner, risikovurderinger, driftsrutiner, avvik og hvordan de håndteres, ledelsens gjennomgang, databehandleravtaler mv.

5.2 Interne roller og ansvar i virksomheten

Virksomhetens øverste ledelse har ansvaret for å sørge for at virksomheten følger gjeldende krav til informasjonssikkerhet og personvern, og at virksomhetens informasjonsbehandling gir et sikkerhetsnivå som er egnet med hensyn til risikoen og behandlingens art. Dette ansvaret bør ivaretas som en del av arbeidet med virksomhetsstyring og kvalitetsforbedring. Ansvaret inkluderer å sette føringer for vurdering og håndtering av risiko, herunder fastsette kriterier for å akseptere risiko, samt å sørge for velfungerende styring og kontroll. Virksomheten skal dokumentere alle tiltak.

Virksomheten skal definere og dokumentere roller, ansvar og myndighet for informasjonssikkerhet og personvern, inkludert sikkerhets- eller personvernleder, system- og dataeiere, databehandlere, underleverandører og, der det er påkrevd, personvernombud. Hver medarbeider skal kjenne sine egne oppgaver og forstå andres relevante ansvar.

Systematisk og dokumentert internkontroll gir andre aktører tillit til at virksomheten ivaretar informasjonssikkerhet og personvern på en tilfredsstillende måte, reduserer behovet for omfattende individuell due diligence, forenkler tilsyn og muliggjør raskere etablering av delings- og databehandleravtaler.

5.3 Ledelsens gjennomgang

Virksomhetens øverste ledelse skal selv gjennomgå virksomhetens aktiviteter innen informasjonssikkerhet og personvern minst én gang i året i tråd med anbefalinger fra Digdir[3] og Datatilsynet[4].

Gjennomgangen kan i tillegg være nødvendig ved:

- endringer i behandlinger av personopplysninger (artikkel 30-protokoll)
- endringer i organiseringen av arbeidet
- resultat fra risikovurderinger og personvernkonsekvensvurderinger som viser eller avdekker at behandlingen er forbundet med høy risiko for den registrerte
- resultat av avviksbehandling
- oppfølging av leverandører og databehandleravtaler
- endring i akseptabel risiko mv.

5.4 Personvernombud

Offentlige virksomheters øverste ledelse skal sørge for at det utpekes et personvernombud. For en privat virksomhet skal øverste ledelse utpeke et personvernombud når informasjonsbehandlingens omfang, art

[3] https://www.digdir.no/informasjonssikkerhet/ledelsens-styring-og-oppfolging/3044
[4] https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/informasjonssikkerhet-internkontroll/etablere-internkontroll/iverksette-styringssystem-for-informasjonssikkerhet/

og formål krever det. Dette gjelder også små virksomheter. Personvernombudet kan være ansatt i virksomheten eller ekstern og utføre oppgavene på grunnlag av en tjenesteavtale.

I tillegg til å være et kontaktpunkt for de registrerte, har personvernombudet både en rådgivende og kontrollerende rolle i virksomheten. Det ligger innenfor den behandlingsansvarliges plikter å sørge for at personvernombudet involveres på riktig måte og til rett tid om alle spørsmål som gjelder vern av personopplysninger. Personvernombudet skal også kontrollere at virksomheten overholder reglene i forordningen. Samlet skal dette sørge for at de registrertes rettigheter ivaretas på en best mulig måte.

Personvernombudet skal gis tilstrekkelige ressurser og tilgang på relevant kompetanse til å utføre sine plikter. Ombudet skal ikke ha interessekonflikt med eventuelle andre roller som vedkommende har i virksomheten, og skal ikke motta instruksjoner om hvordan oppgavene skal utføres.

5.5 Medarbeidere, kompetanse og holdningsskapende arbeid

Alle medarbeidere skal gjøres kjent med kravene til informasjonssikkerhet og personvern, og virksomheten skal beskrive i sitt styringssystem hvordan denne bevisstgjøringen og opplæringen gjennomføres og dokumenteres. Arbeidsavtalen – eller annen skriftlig avtale – skal presisere den ansattes plikt til å følge interne retningslinjer og instrukser for informasjonssikkerhet, personvern og taushetsplikt. Taushetsplikten kan innarbeides direkte i arbeidsavtalen eller dokumenteres gjennom en separat taushetserklæring. Virksomheten skal også ha klare retningslinjer for privat bruk av informasjonssystemer og utstyr.

5.6 Behandlingsprotokoll

Virksomheten skal føre og vedlikeholde en oppdatert behandlingsprotokoll i samsvar med personvernforordningen artikkel 30. Protokollen skal beskrive, for hver behandlingsaktivitet, formålene med behandlingen, kategoriene av registrerte og opplysninger, behandlingsgrunnlag, mottakere og eventuelle overføringer til tredjeland, planlagte tidsfrister for sletting eller anonymisering, og dersom det er mulig, en generell beskrivelse av de tekniske og organisatoriske sikkerhetstiltakene nevnt i artikkel 32 nr. 1. Protokollen skal også angi ansvarlig enhet, kontaktpunkt for personvern og, der det er relevant, henvisning til utførte konsekvens-vurderinger og risikovurderinger.

Databehandlere skal føre en tilsvarende protokoll som minst inneholder navn og kontaktopplysninger til oppdragsgivere, kategorier av behandlinger som utføres på deres vegne, eventuelle overføringer til tredjeland og en beskrivelse av sikkerhetstiltakene. Der virksomheten både er behandlingsansvarlig og databehandler, skal dette fremgå tydelig i samme dokument eller i to atskilte deler av protokollen.

Protokollen skal være lett tilgjengelig for ledelsen, personvernombudet og relevante fagpersoner og kontrollorganer, og den skal kunne fremlegges uten ugrunnet opphold på anmodning fra Datatilsynet. Ansvar for oppdatering skal være tydelig delegert; justeringer skal gjennomføres før nye behandlinger igangsettes eller når endringer i formål, omfang, systemarkitektur eller rettslig grunnlag oppstår.

Virksomheten skal jevnlig kontrollere at opplysningene i protokollen samsvarer med faktisk praksis, og protokollen skal inngå som datagrunnlag i virksomhetens risikostyring, internkontroll og revisjoner.

5.7 Vurdering av personvernkonsekvenser

Virksomheter skal alltid vurdere hvilke konsekvenser behandling av personopplysninger medfører for den registrerte. Virksomheten skal dokumentere lovligheten av behandlingen, formålet, hvordan personvernet til den registrerte er ivaretatt, og at det er gjort tilstrekkelige tiltak for å håndtere risikoen.

Hvis det er sannsynlig at en behandling medfører høy risiko for de registrerte, skal virksomheten gjennomføre en mer grundig personvernkonsekvensvurdering (DPIA).

Etter GDPR artikkel 35 nr. 3 er det behandlingsaktiviteter som alltid krever at det gjennomføres en personvernkonsekvensvurdering.

Virksomhetenes personvernkonsekvensvurdering skal minst inneholde:

- en systematisk beskrivelse av behandlingsaktiviteten
- beskrivelse av formålet med behandlingen av personopplysninger
- en vurdering av om behandlingene av personopplysninger er nødvendige og står i rimelig forhold til formålet
- en vurdering av risikoen for personvernet til den registrerte
- planlagte risikoreduserende tiltak for ivaretakelse av personvernet

Det skal planlegges tiltak som reduserer risikoen for personvernet. Dersom behandlingen av personopplysninger medfører en høy risiko som ikke kan reduseres ved hjelp av rimelige tiltak, skal den behandlingsansvarlige be om forhåndsdrøftelse med Datatilsynet før behandlingen av opplysningene starter.

5.8 Innebygd personvern

Innebygd personvern er et sentralt krav i personvernforordningen. Virksomheten som behandlingsansvarlig og dens leverandører, skal stille krav til og ta hensyn til personvern i alle utviklingsfaser av et system eller en løsning. Virksomheten skal sørge for at informasjonssystemene oppfyller personvernprinsippene, og at de ivaretar de registrertes rettigheter.

Videre er det et krav at personverninnstillinger er satt slik at de i størst mulig grad ivaretar den registrerte. Samtykker kan ikke være krysset av per default, cookies (informasjonskapsler) skal ikke settes med mindre den registrerte aktivt velger det og at samtykke er gyldig etter personvernforordningen. Les mer om dette i Datatilsynets veileder.[5]

5.9 Valg av databehandlere

Når en behandlingsansvarlig velger databehandler eller underleverandør, skal behandlingsansvarlig før avtaleinngåelse vurdere om leverandøren gir tilstrekkelige garantier for å gjennomføre egnede tekniske og organisatoriske tiltak i samsvar med personvernforordningen artikkel 28. Behandlingsansvarlig skal videre inngå en skriftlig databehandleravtale som tydelig angir hvilke personopplysninger som skal behandles, formålene med behandlingen og hvilke behandlinger databehandleren og eventuelle underleverandører skal utføre. Avtalen skal fastsette krav til informasjonssikkerhet, revisjon, bruk av underleverandører og sletting eller tilbakelevering av data ved avtalens opphør. I henhold til artikkel 28 nr. 3 bokstav h oppstilles det krav om at revisjonsmulighet skal reguleres i databehandleravtalen. Behandlingsansvarlig har ansvar for å følge opp databehandlere iht GDPR artikkel 24 og 32, og beror på en vurdering av risiko for brudd på forpliktelser i henhold til avtalen.

Avtalen bør angi behandlingsformål, kategorier av personopplysninger, varighet, tekniske og organisatoriske tiltak, regler for underdatabehandlere, prosedyre for hendelsesvarsling samt krav til sletting eller tilbakelevering av data ved avtalens opphør. Dersom behandlingen innebærer lagring eller tilgang utenfor EØS, må overføringen være basert på et gyldig grunnlag etter kapittel V i GDPR, supplert med nødvendige beskyttelsestiltak.

Leverandører som håndterer data med høy risiko for de registrerte følges opp gjennom periodiske revisjoner, stikkprøver av logg- og tilgangsstyring og krav om rapportering av sikkerhets-brudd uten

[5] https://www.datatilsynet.no/personvern-pa-ulike-omrader/internett-og-apper/bruk-av-informasjonskapsler-og-andre-sporingsteknologier/

ugrunnet opphold. Vesentlige endringer i tjenesten eller hos leverandøren krever ny vurdering av sikkerhetstiltak og, om nødvendig, revisjon av avtalevilkårene. Slik bevarer virksomheten kontrollen over personopplysninger, selv når deler av behandlingen skjer hos eksterne aktører.

5.10 Håndtering av brudd på personopplysningssikkerheten

5.10.1 Brudd som ikke er meldepliktige til Datatilsynet

De fleste brudd på personopplysningssikkerheten vil ikke være meldepliktige fordi de ikke innebærer risiko for de registrertes rettigheter og friheter. Slike brudd skal likevel håndteres systematisk internt.

I henhold til personvernforordningen artikkel 33 nr. 5 skal alle brudd på personopplysningssikkerheten dokumenteres, uavhengig av om de meldes til Datatilsynet eller ikke. Dokumentasjonen skal gjøre det mulig for tilsynsmyndigheten å kontrollere at vurderingene og håndteringen har vært i samsvar med regelverket.

Intern håndtering bør som minimum omfatte:

- registrering av hendelsen og tidspunkt for når virksomheten ble kjent med bruddet,
- en vurdering av årsak, omfang og hvilke personopplysninger som er berørt,
- en begrunnet risikovurdering som viser hvorfor bruddet ikke anses meldepliktig,
- beskrivelse av iverksatte eller planlagte tiltak for å hindre gjentakelse.

Slike vurderinger og tiltak bør inngå som del av virksomhetens internkontroll for personvern og informasjonssikkerhet, og kan også gi grunnlag for forbedring av rutiner, tekniske tiltak eller opplæring.

5.10.2 Meldingspliktige brudd

Melding til Datatilsynet skal inneholde de opplysningene som fremgår av artikkel 33 nr. 3, herunder:

- bruddets art og omfang, inkludert omtrentlig antall berørte registrerte og kategorier av personopplysninger,
- navn og kontaktopplysninger til personvernombud eller annet kontaktpunkt,
- en beskrivelse av de sannsynlige konsekvensene av bruddet for de registrerte,
- en beskrivelse av tiltak som er truffet eller foreslått for å håndtere bruddet og begrense eventuelle negative virkninger.

Dersom bruddet sannsynligvis vil medføre høy risiko for de registrertes rettigheter og friheter, skal de registrerte varsles uten ugrunnet opphold, jf. artikkel 34. Informasjonen skal gis i et klart og forståelig språk. Dersom individuell varsling innebærer uforholdsmessig stor innsats, kan virksomheten benytte offentlig kommunikasjon eller tilsvarende tiltak, forutsatt at informasjonen når de registrerte på en effektiv måte.

5.10.3 Underretting til den registrerte

Dersom det er sannsynlig at avviket har eller vil føre til høy risiko for den registrerte, skal virksomheten underrette vedkommende.

Virksomheten skal som minimum gi den registrerte følgende informasjon:

- Beskrivelse av bruddet
- Navn og kontaktinformasjon til personvernombudet eller et annet kontaktpunkt der mer informasjon kan innhentes

- Beskrivelse av de sannsynlige konsekvensene av bruddet
- Beskrivelse av de tiltakene som virksomheten har truffet eller foreslår å sette i gang for å håndtere bruddet, inkludert (dersom det er relevant) tiltak for å redusere eventuelle skadevirkninger som følge av bruddet

Virksomheten bør så langt det er mulig, ta direkte kontakt med den registrerte. Dersom avviket gjelder mange registrerte og avviket har lav konsekvens for den registrerte, kan informasjon gis gjennom offentlige kanaler.

5.11 Risikovurderinger av KI-løsninger

Virksomheten skal gjennomføre en dokumentert risikovurdering før utvikling, anskaffelse eller drift av KI-systemer. Frem til KI-forordningen er innlemmet i EØS-avtalen og gjennomført i norsk rett, foreligger det ikke en rettslig forpliktelse etter denne forordningen. Anbefalingene i dette punktet er likevel basert på KI-forordningens risikoklassifisering (artikkel 6), da denne er forventet å få virkning for norske virksomheter. Virksomheter bør følge utviklingen nøye.

Der personopplysninger inngår som treningsdata, inndata eller utdata, skal virksomheten i tillegg overholde alle krav i personvernforordningen. Dette innebærer blant annet å:

- vurdere behandlingsgrunnlag og formål med KI-behandlingen,
- gjennomføre en personvern-konsekvensvurdering (DPIA) når vilkårene i artikkel 35 er oppfylt,
- beskrive KI-behandlingen i behandlingsprotokollen, og
- sørge for at informasjon til de registrerte omfatter formål, datakilder, algoritmisk logikk og eventuelle betydelige konsekvenser for den registrerte.

Hvis KI-systemet foretar eller begrunner avgjørelser som kan ha rettslig eller tilsvarende vesentlig betydning for den registrerte, skal virksomheten sikre at avgjørelsen ikke er utelukkende basert på automatisert behandling uten menneskelig innblanding, med mindre vilkårene i personvernforordningen artikkel 22 nr. 2 er oppfylt. Virksomheten skal da etablere manuelle rutiner som gjør det mulig å overprøve avgjørelsen, gi den registrerte mulighet til å uttrykke sitt synspunkt og bestride resultatet.

Risikovurderingen skal vurderes på nytt ved vesentlige endringer i algoritmen, datagrunnlaget, bruksområdet eller det rettslige rammeverket. Resultater og forbedringstiltak fra vurderingen skal inngå i virksomhetens styringssystem for informasjonssikkerhet og personvern.

5.12 Særlig om IoT, sensorer, billetteringsteknologi

Bruken av IoT-enheter, sensorer og billetteringsteknologi i samferdselssektoren innebærer at store mengder data genereres og behandles tett på den enkelte reisende og på kritisk infrastruktur. Slike teknologier kan omfatte alt fra passasjertellere, sanntidssensorer, kamera- og lydsensorer, posisjonsmoduler, adgangs- og valideringsutstyr, kjøretøysensorikk og annet utstyr som kontinuerlig samler inn eller overfører data.

IoT-løsninger skiller seg fra tradisjonelle IT-systemer ved at de ofte er fysisk plassert ute i transportinfrastrukturen, har lang levetid, oppdateres sjeldnere, og kan ha begrensede sikkerhetsmekanismer. Dette krever særskilt oppmerksomhet ved både anskaffelse, drift, integrasjon og utfasing.

6 Deling og datasamarbeid

6.1 Innledning

Deling av data mellom virksomheter i samferdselssektoren bør gjennomføres som en kontrollert prosess, og ikke som en isolert teknisk eller operativ handling. Virksomheten bør kunne dokumentere hva som deles, hvorfor det deles, på hvilket rettslig grunnlag og med hvilken risiko.

Anbefalt prosess for vurdering av datadeling:

1. Avklar delingssituasjonen: hvem er avsender/mottaker, hvilken type tilgang/utlevering, og hvilket formål.
2. Klassifiser datasettet (punkt 6.2).
3. Vurder personvern dersom datasettet inneholder personopplysninger (punkt 6.3-6.4).
4. Vurder taushetsplikt (punkt 6.5).
5. Vurder forretningshemmeligheter, rettigheter og avtalebaserte begrensninger (punkt 6.6).
6. Sikre notoritet, oppfølging og endringshåndtering (punkt 6.7)

Mal for delingsprosess

Vurderingene i kapittel 6.2–6.7 nedenfor bør gjennomføres samlet og dokumenteres ved bruk av *M06 – mal for deling av data.*

6.2 Klassifisering av data

6.2.1 Minimumsbeskrivelse av datasettet

Før virksomheten klassifiserer, bør den beskrive datasettet kort og konkret. Som minimum bør følgende avklares og dokumenteres:

- datasettets navn og avgrensning (hvilke tabeller/variabler/registre inngår)
- kilde og dataeier (hvem har etablert datasettet og hvem forvalter det)
- tidsperiode og oppdatering (historikk, sanntid, frekvens)
- format og tilgangsform (filuttrekk, API, løpende strøm, innsynsløsning)
- volum og detaljeringsnivå (hvor presist, hvor tett på individ/nivå)
- mottaker og mottakerkrets (én mottaker eller flere, videre deling mulig/ikke)
- formål (hva data skal brukes til)

6.2.2 Klassifisering

Ved klassifiseringen bør virksomheten som et minimum vurdere om datasettet:

- inneholder personopplysninger (inkludert opplysninger som kan bli personopplysninger ved sammenstilling), herunder om de er omfattet av GDPR artikkel 9 og/eller 10
- inneholder opplysninger som kan være underlagt taushetsplikt
- inneholder opplysninger som er underlagt graderings- eller skjermingskrav, herunder etter sikkerhetsloven eller interne sikkerhetsinstrukser
- inneholder forretningshemmeligheter eller andre kommersielt sensitive opplysninger
- inneholder rettighetsbelagte data eller avtalebaserte begrensninger
- helt eller delvis er omfattet av krav eller forventninger om tilgjengeliggjøring, for eksempel som åpne data og/eller datasett med høy verdi (HVD), eller av sektorregelverk slik som ITS/MMTIS.

Dersom flere kategorier gjør seg gjeldende samtidig, må vurderingene ses i sammenheng. Det mest restriktive regelsettet eller risikoforholdet (f.eks. taushetsplikt eller høy reidentifiseringsrisiko) vil typisk være styrende for om og hvordan deling kan skje.

Dersom datasettet endres over tid, eller delingen får et annet formål enn opprinnelig forutsatt, bør klassifiseringen vurderes på nytt.

6.2.3 Klassifisering ved behandling av personopplysninger

I klassifiseringen bør virksomheten eksplisitt vurdere om data kan knyttes til enkeltpersoner, enten direkte eller indirekte. Praktiske kjennetegn som ofte øker identifiserbarhet:

- unike identifikatorer (kunde-ID, enhets-ID, kortnummer, brukernavn)
- posisjon og bevegelsesmønstre (særlig over tid)
- tidsstempler med høy presisjon
- kombinasjoner av «tilsynelatende uskyldige» opplysninger (f.eks. tid + sted + rute)

6.2.4 Om datasettet er underlagt andre begrensninger

I tillegg til personopplysninger bør virksomheten kartlegge om datasettet inneholder:

- opplysninger som kan være taushetsbelagte
- opplysninger som kan være graderte eller skjermingsverdige av hensyn til nasjonal sikkerhet, samfunnssikkerhet eller beredskap
- opplysninger som kan være konkurransesensitive eller forretningskritiske
- data som helt eller delvis kan være underlagt lisensvilkår, avtaleforpliktelser eller tredjepartsrettigheter

6.2.5 Klassifiseringskonklusjon (resultat)

Klassifiseringen bør ende i en kort konklusjon som minst sier:

- hvilke kategorier som gjelder
- hvilke deler av datasettet som er «mest kritiske» (f.eks. bestemte variabler)
- hvilke føringer dette gir for videre vurderinger (f.eks. at deling må skje pseudonymisert, aggregert eller ikke kan skje)

Klassifiseringen bør oppdateres hvis datasettet, formålet, mottakerforholdet eller tilgangsformen endres.

6.3 Vurdering av data som er eller inneholder personopplysninger

6.3.1 Overordnet

Virksomheten bør gjennomføre en samlet vurdering av om og hvordan opplysningene kan deles i samsvar med personvernregelverket. Vurderingen tar utgangspunkt i klassifiseringen etter punkt 6.2, og gjennomføres basert på de temaene som er beskrevet i punkt 6.3.2 til 6.3.7. Virksomheten bør som et minimum:

- avklare formålet med delingen og hvilke konkrete leveranser/analyser mottaker skal gjennomføre
- vurdere om delingen kan skje innenfor opprinnelig formål, eller om delingen i realiteten innebærer et nytt formål (viderebruk)
- ta stilling til hvilket behandlingsgrunnlag delingen kan baseres på
- avklare roller og ansvar mellom avsender og mottaker
- avklare hvordan informasjonsplikt overfor registrerte er ivaretatt eller skal ivaretas
- kartlegge hvilke systemer og tekniske løsninger som inngår i delingen, og vurdere behov for oppdatert risikovurdering og eventuelt personvernkonsekvensvurdering (DPIA)

6.3.2 Forholdet til opprinnelig innsamling og behandlingsgrunnlag

Ved deling av personopplysninger må virksomheten ta utgangspunkt i rammene som følger av den opprinnelige innsamlingen. Dette gjelder uavhengig av om opplysningene deles internt mellom virksomheter i samme konsern eller utleveres til eksterne aktører.

I denne vurderingen må virksomheten ta stilling til:

- hvilket formål opplysningene opprinnelig ble samlet inn for
- hvilket behandlingsgrunnlag den opprinnelige behandlingen bygget på
- om deling med aktuelle mottakere var forutsatt, kommunisert eller fremstår som en naturlig del av den opprinnelige behandlingen
- om delingen innebærer endringer som typisk øker risiko, for eksempel:
  - flere eller nye mottakere
  - mer detaljerte data enn tidligere (økt presisjon, flere variabler, lengre historikk)
  - lengre lagringstid
  - nye sammenstillinger eller koblinger
  - løpende tilgang i stedet for enkel utlevering

Hvis delingen ligger innenfor det opprinnelige formålet og rammene fra innsamlingen, kan deling i mange tilfeller være mulig, forutsatt at øvrige krav og risikoreduserende tiltak håndteres.

Dersom personopplysningene er samlet inn på grunnlag av samtykke, må virksomheten vurdere om samtykket også dekker deling, eller om nytt samtykke må innhentes. Dersom behandlingen bygger på lov, avtale eller oppgave i allmennhetens interesse, må det tilsvarende vurderes om dette behandlingsgrunnlaget gir adgang til deling.

6.3.3 Innsamlingsmåte (direkte/indirekte) og håndtering av informasjonsplikt

Virksomheten bør alltid avklare hvordan opplysningene ble samlet inn, fordi dette påvirker hvordan informasjon til de registrerte bør håndteres.

Direkte innsamling (jf. GDPR artikkel 13)

Virksomheten bør kontrollere at informasjonen som ble gitt ved innsamlingen (f.eks. i personvernerklæring, vilkår, app-tekst, skjema) dekker:

- at opplysningene kan deles
- formålet med delingen
- mottaker eller mottakerkategori
- hovedtrekk ved lagringstid og
- de registrertes rettigheter/kontaktpunkt

Hvis delingen ikke er dekket, bør virksomheten vurdere behov for supplerende informasjon før delingen etableres eller endres (jf. artikkel 13 nr. 3).

Indirekte innsamling (jf. GDPR artikkel 14)

Virksomheten bør avklare om og hvordan de registrerte har fått informasjon om at opplysningene behandles, hvor de kommer fra, og at de kan deles videre.

Dersom informasjonsplikten ikke er oppfylt, bør virksomheten planlegge hvordan informasjon kan gis på en egnet måte, i tråd med artikkel 14, herunder innenfor de fristene som følger av artikkel 14 nr. 3 og med hensyn til eventuelle unntak etter artikkel 14 nr. 5.

Hva virksomheten normalt bør informere om ved ny eller endret deling

Når deling etableres eller endres, bør virksomheten vurdere om de registrerte skal informeres i samsvar med personvernforordningen artikkel 12, 13 og 14.

Avhengig av hvordan opplysningene er samlet inn, kan dette blant annet omfatte informasjon om:

- hvilke typer opplysninger som deles
- formålet med delingen
- hvem som mottar opplysningene (eller mottakerkategori)
- hvor lenge opplysningene vil være tilgjengelige hos mottaker
- de viktigste rettighetene og hvem de registrerte kan kontakte

Praktisk gjennomføring når individuell informasjon er krevende

Dersom det er svært mange registrerte og individuell informasjon fremstår som lite praktisk, kan virksomheten vurdere alternative informasjonskanaler som likevel sikrer at informasjonen er lett tilgjengelig og forståelig.

Valgt løsning må være egnet til å ivareta kravene i artikkel 12, og virksomheten bør dokumentere vurderingen, herunder hvorfor løsningen anses forsvarlig og når informasjonen ble gjort tilgjengelig.

6.3.4 Viderebruk og forenlighet

Viderebruk av personopplysninger innebærer at opplysningene brukes til et annet formål enn det de opprinnelig ble samlet inn for. Etter personvernforordningen artikkel 6 nr. 4 kan viderebruk skje på to måter:

- dersom viderebruken har eget rettslig grunnlag, for eksempel i lov eller samtykke, eller
- dersom viderebruken kan anses som forenlig med det opprinnelige formålet.

Ved vurderingen av forenlighet bør virksomheten ta utgangspunkt i kriteriene i artikkel 6 nr. 4, herunder blant annet:

- sammenhengen mellom det opprinnelige formålet og det nye formålet,
- i hvilken kontekst opplysningene ble samlet inn,
- opplysningenes art og eventuelle særskilte risikoer,
- mulige konsekvenser for de registrerte,
- om det foreligger egnede garantier, som pseudonymisering eller andre risikoreduserende tiltak.

Viderebruk til arkivformål i allmennhetens interesse, vitenskapelig eller historisk forskning eller statistiske formål anses ikke som uforenlig med det opprinnelige formålet, forutsatt at kravene i artikkel 89 er oppfylt.

Dersom viderebruken ikke er forenlig og det ikke foreligger eget rettslig grunnlag, bør personopplysningene ikke viderebrukes i identifiserbar form.

6.3.5 Rollevurdering ved deling av personopplysninger

Før personopplysninger deles, må virksomheten avklare hvilken rolle mottakeren har etter personvernregelverket. Dette omfatter om mottakeren er selvstendig behandlingsansvarlig, felles behandlingsansvarlig eller databehandler.

Dersom mottakeren fastsetter egne formål med behandlingen eller kombinerer dataene med egne datasett, vil mottakeren som hovedregel være selvstendig behandlingsansvarlig. Bruk av egen databehandler utgjør derimot ikke deling, men er formelt sett en del av virksomhetens egen behandling.

Dersom delingen innebærer at avsender og mottaker i fellesskap fastsetter formål og midler, må det foreligge en avtale om felles behandlingsansvar i tråd med personvernforordningen artikkel 26.

Partene bør i tillegg ha en bevissthet om mottakerens virksomhetstype (forvaltningsorgan, statlig eller kommunalt selskap, privat virksomhet mv.), ettersom dette kan utløse særskilte plikter etter annet regelverk, som offentleglova, arkivloven, forvaltningsloven eller sikkerhetsregelverk.

Klar rolleavklaring før deling reduserer risiko for rettslige uklarheter, og er en forutsetning for korrekt avtaleverk, nødvendig dokumentasjon og etterlevelse av personvernregelverket.

6.3.6 Særlig om utlevering av personopplysninger til statistikkformål hos mottaker

Det følger av artikkel 5 første ledd bokstav b at viderebehandling til statistiske formål er forenlig viderebruk, såfremt behandlingsansvarlig sørger for tilstrekkelige garantier i henhold til GDPR artikkel 89.

Ved vurderingen av om personopplysninger kan overføres til en mottaker for statistikkformål, bør virksomheten undersøke hvorvidt mottakeren har et statistisk formål med behandlingen som er knyttet til offentlig myndighetsutøvelse eller annen oppgave av allmenn interesse. I så fall vil mottakeren typisk kunne behandle personopplysninger i medhold av personopplysningsloven § 8, forutsatt at behandlingen skjer med egnede garantier i tråd med GDPR artikkel 89. Det innebærer typisk at opplysningene minimeres og anonymiseres så langt dette er forenlig med formålet. Der anonymisering ikke lar seg gjennomføre uten at det hindrer oppfyllelsen av det statistiske formålet, kan pseudonymisering benyttes som alternativt tiltak.

Dersom mottakeren er et offentlig statistikkinstitutt eller annen aktør som har lovpålagt rapporteringsoppgave, vil GDPR artikkel 6 nr. 1 bokstav c eller e normalt gi behandlingsgrunnlaget. I andre tilfeller må virksomheten vurdere om samtykke eller særskilt sektorlovgivning er mer egnet. Risiko for gjenidentifisering bør vurderes, og vurderingen bør innarbeides i en oppdatering av gjeldende personvernkonsekvensvurdering før utleveringen finner sted.

Før første overføring oppdaterer virksomheten sin behandlingsprotokoll med referanse til statistikkhjemmel, valgt anonymiserings- eller pseudonymiseringsmetode og mottakers kontaktpunkt. Personvernerklæringen opplyser samtidig at opplysningene inngår i statistikk som ikke har direkte konsekvenser for den enkelte. Etter at delingen er etablert, skal avsender jevnlig følge opp at mottaker sletter eller anonymiserer identifiserbare data når formålet er oppfylt.

6.3.7 Systemer, dataflyt og behov for risikovurdering/DPIA

Ved deling av personopplysninger bør virksomheten kartlegge hvilke systemer og tekniske løsninger som inngår i delingen, fordi endringer i tilgangsmodell, systemarkitektur eller behandlingsmåte kan påvirke risiko og dokumentasjonsbehov.

Virksomheten bør som minimum:

- beskrive dataflyten fra kildesystem til mottaker (inkludert mellomlagring, integrasjoner/API, analyseplattformer, driftsleverandører og eventuelle underleverandører)
- avklare hvor data lagres og behandles, og hvem som har tilgang i hvert ledd
- avklare om delingen innebærer nye tekniske komponenter eller nye behandlingsmåter (f.eks. løpende strøm i stedet for engangsuttrekk, skyplattform, nye sammenstillinger)
- vurdere om delingen innebærer vesentlig endring i risiko, slik at risikovurderinger må oppdateres
- vurdere om delingen utløser behov for ny eller oppdatert personvernkonsekvensvurdering (DPIA), særlig der delingen innebærer:
    - systematisk og omfattende behandling (volum/løpende deling)
    - bruk av detaljerte lokasjons-/bevegelsesdata over tid
    - nye sammenstillinger som gir økt innsikt om enkeltpersoner
    - nye mottakere eller ny tilgangsmodell som øker eksponeringsrisiko

6.4 Tiltak ved deling av personopplysninger

Deling av personopplysninger i identifiserbar form forutsetter at det foreligger et behandlingsgrunnlag etter personvernforordningen artikkel 6. I mange tilfeller vil også deling i identifiserbar form forutsette at det iverksettes tekniske og organisatoriske tiltak som begrenser datamengden, reduserer identifiserbarhet og sikrer tilstrekkelig kontroll med videre bruk hos mottaker. Tiltakene må vurderes konkret i lys av formålet med delingen, opplysningenes art og risikoen for de registrerte.

Aktuelle tiltak er:

- begrensning av datamengde og detaljeringsnivå (dataminimering),
- pseudonymisering eller anonymisering,
- tilgangsstyring og logging hos mottaker,
- begrensninger i lagringstid og sammenstilling,
- andre avtalemessige og organisatoriske tiltak som tydeliggjør ansvar og plikter.

Tiltakene bør dokumenteres som del av virksomhetens vurderinger, og inngå i eventuelle avtaler eller delingsprotokoller.

Pseudonymisering

Pseudonymisering innebærer at identifiserende opplysninger erstattes med pseudonymer eller koder, slik at enkeltpersoner ikke kan identifiseres uten bruk av tilleggsinformasjon som holdes atskilt. Pseudonymiserte opplysninger er fortsatt personopplysninger og omfattes fullt ut av personvernregelverket.

Pseudonymisering kan være et egnet tiltak for å redusere risiko ved deling, særlig der full anonymisering ikke er mulig uten at formålet med delingen undergraves. Samtidig må virksomheten være oppmerksom på at:

- deling av pseudonymiserte opplysninger fortsatt krever behandlingsgrunnlag,
- mottakers mulighet til å reidentifisere, herunder gjennom sammenstilling med egne data, må vurderes,
- pseudonymiserte data ikke kan anses som anonymiserte dersom reidentifisering er mulig, selv i teorien.

Anonymisering

Anonymisering innebærer at opplysninger behandles slik at enkeltpersoner ikke lenger kan identifiseres, verken direkte eller indirekte. Anonymiserte opplysninger er ikke personopplysninger, og behandlingen faller utenfor personvernregelverket.

For at opplysninger skal anses som anonymiserte, må alle identifikatorer fjernes eller endres på en måte som gjør at enkeltpersoner ikke lenger kan identifiseres, verken direkte eller indirekte, også ved sammenstilling med andre tilgjengelige datakilder. Dette forutsetter en konkret vurdering av risiko, herunder:

- risiko for kobling til andre datasett (linkage),
- risiko for utledning av egenskaper (inference),
- risiko for å isolere enkeltpersoner (singling-out).

Valg av anonymiseringsteknikk må tilpasses datasettet og formålet med bruken, og bør dokumenteres som del av virksomhetens risikovurdering.

Nærmere omtale av pseudonymisering og anonymisering, herunder relevante teknikker og risikovurderinger, følger i eget temaark (T03 – Hva er en personopplysning).

6.5 Håndtering av taushetsbelagte og konfidensielle opplysninger

6.5.1 Overordnet

Dersom et datasett helt eller delvis inneholder opplysninger som kan være underlagt taushetsplikt, bør dette avklares tidlig i delingsprosessen og før det tas stilling til øvrige vilkår for deling. Taushetsplikt kan utgjøre en selvstendig og avgjørende begrensning for deling, også der delingen ellers fremstår som forsvarlig etter personvernregelverket.

I vurderingen bør virksomheten som minimum:

- identifisere hvilke deler av datasettet som er (eller kan være) taushetsbelagt, og hva som gjør dem taushetsbelagte
- avklare om deling i det hele tatt er tillatt, og i så fall på hvilke vilkår
- vurdere om mottakers behov kan dekkes med mindre inngripende tiltak (for eksempel aggregering, anonymisering eller fjerning av variabler)
- dokumentere vurderingen og beslutningen, inkludert hvilke opplysninger som deles og hvilke som holdes tilbake

Virksomheten må ta utgangspunkt i om den selv (og eventuelt mottaker) er en offentlig eller privat virksomhet, og hvilke regelsett som dermed kan komme til anvendelse. For offentlige virksomheter har det betydning om virksomheten opptrer som forvaltningsorgan eller ikke, herunder at taushetsplikt typisk følger av forvaltningsloven og/eller sektorlovgivning. Se nedenfor om offentlige virksomheter som ikke er forvaltningsorganer etter forvaltningsloven.

For private virksomheter vil begrensninger i deling typisk følge av forretningshemmelighetsloven og avtalebaserte konfidensialitetsforpliktelser.

Eksempel på taushetsbelagte eller konfidensielle opplysninger: Forretningshemmeligheter

Forretningshemmeligheter er typisk kommersielt sensitive opplysninger, herunder drifts- eller forretningsforhold, som det vil være av konkurransemessig betydning å hemmeligholde. Det vises i denne forbindelse til forvaltningsloven § 13 (1) nr 2 og forretningshemmelighetsloven § 2. I samferdselssektoren vil dette i praksis ofte være knyttet til følgende data:

- Salgs-/billettdata per avgang/linje/kunde: kjøp, rabatt, kanal og bruksmønster.
- Pris- og rabattmodeller knyttet til segmenter/enkeltkunder
- Drifts- og regularitetsdata på operatørnivå
- Kundeservice-/reklamasjonsdata

6.5.2 Lovbestemt taushetsplikt

Offentlige forvaltningsorganer og offentlige virksomheter kan være underlagt lovbestemt taushetsplikt etter blant annet forvaltningsloven, sikkerhetsloven og sektorlovgivning, og vil samtidig være omfattet av innsynsregler etter offentleglova. Slike regler setter rammer for hvilke opplysninger som kan deles, med hvem og til hvilket formål.

Før deling bør organet eller virksomheten særlig vurdere:

- om datasettet inneholder opplysninger som ikke kan deles med den aktuelle mottakeren
- om det finnes et uttrykkelig rettslig grunnlag som gir adgang til deling (for eksempel særlige delingshjemler i sektorregelverk)
- om deling kan skje som ledd i mottakers lovpålagte oppgaver (der det er relevant)
- om deling kan skje i bearbeidet form (for eksempel ved å fjerne identifiserende eller sensitive variabler, redusere presisjon eller bruke terskler)
- om delingen kan innebære at taushetsbelagte opplysninger i praksis blir tilgjengeliggjort gjennom sammenstilling eller små grupper (særlig ved detaljerte tid-/stedsdata)

Der deling er tillatt, bør organet eller virksomheten sikre at delingen er avgrenset til det som er nødvendig for formålet, og at det er kontroll med tilgang, bruk og lagring.

Virksomheten bør være oppmerksom på at taushetspliktreglene og rammene for saksbehandling i forvaltningen er under utvikling, herunder at det er vedtatt ny forvaltningslov som skal erstatte dagens lov. Ved løpende datasamarbeid bør virksomheten derfor etablere en praksis for å følge regelverksendringer og vurdere om disse påvirker delingsgrunnlag, vilkår, avtaler og rutiner.

6.5.3 Særlig om offentlige virksomheters forhold til forvaltningsloven

Offentleglova har et videre virkeområde enn forvaltningsloven. Dette innebærer at offentlige virksomheter som ikke er forvaltningsorganer etter forvaltningsloven, typisk er omfattet av innsynsreglene etter offentleglova.

For å unngå at slike virksomheter står uten adgang til å skjerme opplysninger underlagt taushetsplikt, fastsetter offl. § 13 andre ledd at taushetsplikt etter forvaltningsloven kan anvendes tilsvarende. Bestemmelsen gir dermed en adgang, men ikke en plikt, til å unnta opplysninger. Selv om offentleglova gir en adgang til å anvende forvaltningslovens taushetspliktregler, innebærer ikke det at virksomheten står fritt til å dele eller tilgjengeliggjøre opplysninger. Virksomheten må uansett sikre at deling eller tilgjengeliggjøring ikke innebærer utlevering av forretningshemmeligheter eller annen informasjon som er vernet etter forretningshemmelighetsloven.

6.5.4 Anbefalt dokumentasjon ved deling av taushetsbelagte opplysninger

Når deling av taushetsbelagte opplysninger er tillatt, bør virksomheten tydeliggjøre mottakers forpliktelser gjennom avtale eller delingsprotokoll. Dette bør som et minimum omfatte:

- formål og bruksrammer (inkludert hva opplysningene ikke skal brukes til)
- forbud eller klare begrensninger for videre deling/tilgjengeliggjøring
- krav til informasjonssikkerhet (tilgangsstyring, behovsprinsipp, logging, internkontroll)
- lagringstid og krav til sletting/anonymisering
- avvikshåndtering (varsling, håndtering av brudd, kontaktpunkter)
- kontroll og oppfølging (for eksempel stikkprøver, revisjonsrett eller rapportering ved løpende deling)

6.5.5 Forretningshemmeligheter etter forretningshemmelighetsloven

Som nevnt over må forvaltningsorganer ved vurdering av deling av opplysninger først ta stilling til om opplysningene er underlagt taushetsplikt etter forvaltningsloven eller sektorlovgivning.

For offentlige virksomheter som ikke er forvaltningsorganer, og for private virksomheter, er det med tanke på forretningshemmeligheter sentralt å vurdere forpliktelsene etter forretningshemmelighetsloven.

Forretningshemmelighetsloven forbyr urettmessig tilegnelse, bruk og formidling av forretningshemmeligheter. Ved deling av data må organet eller virksomheten derfor vurdere om delingen kan innebære at mottaker får kunnskap om eller rådighet over opplysninger som utgjør forretningshemmeligheter, og om slik deling kan anses urettmessig etter loven.

Ved vurderingen bør det særlig tas stilling til:

- om datasettet inneholder opplysninger som utgjør forretningshemmeligheter, herunder opplysninger som ikke er allment kjent eller lett tilgjengelige, og som har kommersiell verdi fordi de er hemmelige
- om deling vil innebære urettmessig bruk eller formidling av forretningshemmeligheter som virksomheten har fått kunnskap om i anledning av et tjeneste-, tillitsverv- eller forretningsforhold
- om mottaker vil kunne kombinere opplysningene med egne eller andre datasett på en måte som gir tilgang til forretningshemmeligheter
- om deling forutsetter samtykke fra rettighetshaver, eller annet rettslig grunnlag som gjør bruken eller formidlingen lovlig
- om formålet kan oppnås gjennom bearbeidede data, slik at risikoen for urettmessig tilegnelse, bruk eller formidling reduseres

Dersom konfidensialitetsforpliktelser ikke kan håndteres gjennom nødvendig klarering eller tilstrekkelig bearbeiding, kan datasettet som utgangspunkt ikke deles.

6.6 Håndtering av data underlagt andre rettigheter

6.6.1 Opphavsrett og databaserett

I tillegg til personopplysninger og taushetsplikt kan deling av data være begrenset av andre rettslige rammer, særlig immaterielle rettigheter og avtalebaserte forpliktelser. Slike rettigheter kan utgjøre selvstendige skranker for deling, eller stille vilkår for hvordan deling kan gjennomføres, også der personvernregelverket for øvrig er oppfylt

Datasett, sammenstillinger og strukturer kan være vernet etter åndsverkloven. Dette gjelder særlig der dataene:

- er resultat av en selvstendig skapende innsats (opphavsrett), eller
- inngår i databaser der det er foretatt en vesentlig investering i innsamling, kontroll eller presentasjon (databaserett).

Opphavsrett og databaserett kan begrense både kopiering, viderebruk og tilgjengeliggjøring av data, også når dataene ikke inneholder personopplysninger.

Virksomheten bør derfor vurdere:

- hvem som innehar rettighetene til datasettet eller deler av det,
- om virksomheten selv har tilstrekkelige rettigheter til å dele dataene videre,
- om delingen omfattes av lovbestemte unntak eller begrensninger, eller
- om deling forutsetter samtykke, lisens eller annen tillatelse fra rettighetshaver.

6.6.2 Lisenser, avtaler og tredjepartsrettigheter

Data kan også være underlagt begrensninger som følger av avtale, uavhengig av om dataene i seg selv er rettighetsbelagte. Dette kan blant annet omfatte:

- lisensvilkår fra leverandører eller datatilbydere,
- samarbeidsavtaler, konsesjonsvilkår eller offentlig–privat samarbeid,

- kontraktsfestede konfidensialitets- eller bruksbegrensninger.

Slike avtalebaserte rettigheter kan begrense adgangen til deling, også der det ellers foreligger behandlingsgrunnlag etter personvernregelverket.

Som del av den anbefalte fremgangsmåten bør virksomheten derfor avklare:
- om dataene er underlagt avtalefestede eller tredjepartsbaserte begrensninger,
- om avtalene åpner for viderebruk eller deling til bestemte formål eller mottakere

6.6.3 Konsekvens ved manglende rettighetsavklaring

Dersom det ikke foreligger tilstrekkelig rettslig grunnlag for deling, rettighetene ikke kan klareres, eller beskyttelsesbehovet ikke kan håndteres gjennom bearbeiding av data, bør datasettet som utgangspunkt ikke deles.

Der deling er mulig, bør rettigheter, begrensninger og forutsetninger tydeliggjøres overfor mottaker, for eksempel gjennom avtale eller delingsprotokoll.

6.7 Sikre notoritet

Som del av en forsvarlig delingsprosess anbefales det at virksomheten sikrer tilstrekkelig notoritet rundt de vurderingene og beslutningene som ligger til grunn for delingen. Formålet er å gjøre det etterprøvbart hva som deles, hvorfor det deles, på hvilket grunnlag, og hvilke rammer som gjelder for mottaker. Dette er særlig viktig ved løpende datasamarbeid, deling som skjer over tid, eller der datasettet endrer karakter.

Det anbefales at virksomheten sørger for dokumentasjon som viser:
- hvilket datasett som deles (inkludert versjon/uttrekkstidspunkt, format og ev. presisjonsnivå)
- formål og bruksrammer for delingen (hva mottaker skal bruke dataene til, og ev. hva de ikke skal brukes til)
- klassifiseringen etter punkt 6.2 (personopplysninger, taushetsplikt, forretningshemmeligheter, rettigheter mv.)
- rettslig grunnlag og vurderinger der dette er relevant (særlig for personopplysninger, forenlighet og/eller valgt delingsgrunnlag)
- rolleavklaring etter GDPR (selvstendig behandlingsansvar, felles behandlingsansvar eller databehandler) og nødvendig avtalegrunnlag (art. 26/28 der relevant)
- tiltak og forutsetninger som er lagt til grunn for delingen (for eksempel dataminimering, pseudonymisering/anonymisering, tilgangsstyring, logging, lagringstid og begrensninger i videre utlevering)
- oppfølging og endringshåndtering (hvem som kan endre datasettet, formålet, mottakerkretsen eller teknisk tilgang, og hvordan dette skal dokumenteres)

Notoritet kan for eksempel sikres gjennom avtale og/eller delingsprotokoll, interne beslutningsnotater, oppdatering av behandlingsprotokoll (GDPR art. 30) og relevante risikovurderinger/DPIA der dette er påkrevd eller hensiktsmessig. Ved deling mellom offentlige aktører bør virksomheten samtidig være oppmerksom på at dokumentasjonen kan være gjenstand for innsyn etter offentleglova, og innrettes deretter.

7 Oversikt over gjeldende temaark og maler

7.1 Innledning

Nedenfor følger en oversikt over sentrale eller typiske behandlingsaktiviteter i samferdselssektoren, med tilhørende personopplysningskategorier. Det er utarbeidet temaark og maler for noen ulike kategorier. Noen av temaarkene inneholder generelle føringer på behandlingsaktiviteter som ikke bare knytter seg til samferdselssektoren, mens andre temaark og veiledninger er mer rettet inn mot sektoren. Temaarkene skal hjelpe til å vurdere behandlingen på ulike temaer innenfor samferdselssektoren. Maler er eksempler på hvordan man kan gjennomføre f.eks. en DPIA.

7.2 Temaark

Her følger en oversikt over gjeldende temaark:

- T01 – Forklarende dokument om roller og ansvar i samferdselssektoren
- T02 – Oversikt over sektorlover
- T03 – Hva er en personopplysning
- T04 – Registrertes rettigheter
- T05 – Behandling til statistiske formål
- T06 – Kameraovervåkning
- T07 – Ulykkesdata på veg
- T08 – Utlevering av opplysninger til påtalemyndigheten

7.3 Maler

- M01 – Sjekkliste for etterlevelse av krav innen personvern og informasjonssikkerhet
- M02 – Sjekkliste for risikovurderinger
- M03 – Vurdering av behovet for å gjennomføre DPIA
- M04 – Mal for DPIA
- M05 – Mal for forenlighetsvurdering
- M06 – Mal for deling av data.