## M01 – Sjekkliste for etterlevelse av krav innen personvern og informasjonssikkerhet

| Sjekkliste for etterlevelse av krav innen personvern og informasjonssikkerhet | |
|---|---|
| Versjon | Versjon 1.0 – 29.04.2026 |
| Målgruppe | Virksomheter i samferdselssektoren |
| Rettskilder | Personvernforordningen, personopplysningsloven |

Denne sjekklisten er et praktisk hjelpemiddel for etterlevelse av krav innen personvern og informasjonssikkerhet.

Sjekklisten skal gjøre det enklere å:

- identifisere eventuelle mangler i styringssystemer, rutiner eller tiltak
- dokumentere vurderinger og avklaringer
- tilrettelegge for effektiv gjennomgang i forbindelse med revisjon og internkontroll
- være et hjelpemiddel til vurderinger knyttet datadeling og datakonsumering

Sjekklisten er særlig ment for virksomheter som mangler et dekkende ISMS / internkontrollsystem, som et utgangspunkt for å identifisere hva som bør vurderes for å sikre etterlevelse.

Merk at denne sjekklisten handler om hva virksomheten bør kontrollere internt. Veilederen inneholder også et annet verktøy for hvilke vurderinger som bør gjøres ved deling av data, se i den forbindelse M06 – mal for deling av data.

# Den registrertes rettigheter

| Nr | Sjekkpunkt | Referanse |
|---|---|---|
| 1 | Sikrer virksomheten at den registrerte har innsynsrett i sine personopplysninger, og at dette er dokumentert i rutiner eller verktøy? | Art. 15 (1–3), 12 (3) |
| 2 | Har virksomheten en arbeidsprosess som sørger for at den registrerte får full oversikt over hvilke personopplysninger som behandles, inkludert tilgang fra andre virksomheter? | Art. 15 (1)(c), 15 (2) |
| 3 | Legges det til rette for at samiskspråklige, fremmedspråklige og personer med funksjonsnedsettelser kan utøve innsynsretten, og dokumenteres dette? | Art. 12 (1) |
| 4 | Er det etablert saksflyt, systemstøtte og friststyring som ivaretar gratis innsyn innen 30 dager? | Art. 15 (3), 12 (3) |
| 5 | Sikres retten til sletting når behandlingsgrunnlaget bortfaller, inkludert logging av sletting og vurdering av eventuelle unntak? | Art. 17 (1)(a), 17 (3) |
| 6 | Orienteres den registrerte om klageadgangen dersom krav om retting eller sletting avslås? | Art. 12 (4) |
| 7 | Er det klare rutiner for å informere den registrerte om behandlingens formål og varighet? | Art. 13 (1), 14 (1) |
| 8 | Sikrer virksomheten at overordnet ansvar for ivaretakelse av den registrertes rettigheter er tydelig plassert og dokumentert? | Art. 5 (2) |
| 9 | Har virksomheten en prosess slik at den registrerte enkelt kan trekke tilbake sitt samtykke til behandling av personopplysninger? | Art. 7 (3) |
| 10 | Gis den registrerte informasjon om kontaktopplysninger til behandlingsansvarlig, representant og personvernombud? | Art. 13 (1)(a–b) |
| 11 | Gis den registrerte informasjon om formålene med behandlingen og det rettslige grunnlaget? | Art. 13 (1)(c) |
| 12 | Gis den registrerte informasjon om virksomhetens berettigede interesser dersom behandlingen bygger på art. 6 (1)(f)? | Art. 13 (1)(d) |
| 13 | Gis den registrerte informasjon om mottakere eller kategorier av mottakere av personopplysningene? | Art. 13 (1)(e) |
| 14 | Blir den registrerte informert om eventuelle overføringer til tredjeland og hvilke beskyttelsestiltak som er på plass? | Art. 13 (1)(f), 14 (1)(f), kap. V |
| 15 | Gis den registrerte informasjon om oppbevaringsperioden eller kriteriene for fastsettelse av denne? | Art. 13 (2)(a) |
| 16 | Gis den registrerte informasjon om retten til innsyn, retting, sletting, begrensning, dataportabilitet og protest? | Art. 13 (2)(b), 15–21 |
| 17 | Er det lagt til rette for at den registrerte kan få rettet eller slettet sine personopplysninger, og finnes det en dokumentert prosedyre for dette (ansvar, frister, verifikasjon)? | Art. 16–17 |
| 18 | Gis den registrerte informasjon om retten til å trekke tilbake samtykke dersom behandlingen bygger på samtykke? | Art. 13 (2)(c), 7 (3) |
| 19 | Gis den registrerte informasjon om retten til å klage til tilsynsmyndigheten (Datatilsynet)? | Art. 13 (2)(d) |
| 20 | Gis den registrerte informasjon om automatiserte avgjørelser, inkludert profilering, og om betydningen og konsekvensene av slik behandling? | Art. 22, 13 (2)(f) |
| 21 | Dersom virksomheten har til hensikt å viderebehandle personopplysninger for andre formål, foreligger rutiner for å informere den registrerte? | Art. 13 (3) |
| 22 | Er personvernerklæringen lett tilgjengelig, skrevet på klart og forståelig språk og tilpasset målgruppen? | Art. 12 (1) |
| 23 | Har virksomheten etablert verktøy som muliggjør dataportabilitet til ny behandlingsansvarlig på sikker måte? | Art. 20 (2) |
| 24 | Har virksomheten rutiner for midlertidig begrensning av behandling og for å underrette tredjeparter ved retting, sletting eller begrensning? | Art. 18–19 |
| 25 | Har virksomheten prosess for å sikre menneskelig involvering ved automatisert behandling som har rettsvirkning for den registrerte? | Art. 22 (3) |
| 26 | Sikrer virksomheten at prinsippene om lovlighet, rettferdighet og åpenhet dokumenteres og etterleves i praksis (accountability)? | Art. 5 (1)(a), (2) |

# Tekniske og organisatoriske tiltak

| Nr | Sjekkpunkt | Referanse |
|---|---|---|
| 1 | Er tekniske og organisatoriske tiltak vurdert i forhold til virksomhetens størrelse og risiko? | Art. 24 (1), 32 (1) |
| 2 | Har virksomheten fastsatt nivå for akseptabel risiko og i tråd med egne mål? | — |
| 3 | Er tiltakene basert på grundige risikovurderinger for å sikre et tilstrekkelig sikkerhetsnivå? | Art. 32 (1) |
| 4 | Er tiltakene forholdsmessige med hensyn til virksomhetens behov og risiko? | Art. 24 (1), 32 (1) |
| 5 | Er det etablert et styringssystem for informasjonssikkerhet og personvern som er tilpasset virksomhetens risikobilde? | Art. 24 (1), 25 (1) |
| 6 | Har virksomheten definert akseptabelt risikonivå og etablert nødvendig risikohåndtering? | Art. 24 (1) |
| 7 | Har virksomheten fastsatt regler for håndtering av risiko og oppfølging av tiltak? | Art. 24 (1), 32 (1) |
| 8 | Er ansvarsfordeling mellom ansatte og eksterne aktører klart definert og dokumentert? | Art. 24 (1) |
| 9 | Har øverste leder ansvar for styring og oppfølging av informasjonssikkerhet og personvern, og sørger for etterlevelse? | Art. 24 (1) |
| 10 | Har virksomheten utpekt personvernombud når plikt foreligger? | Art. 37 (1) |
| 11 | Har personvernombudet tilstrekkelige ressurser, uavhengighet og direkte rapporteringslinje til ledelsen? | Art. 38 (2–3,6) |
| 12 | Er roller, ansvar og myndighet tydelig definert og kjent i virksomheten, inkludert beslutningsmatrise? | Art. 24 (1) |
| 13 | Får ansatte regelmessig opplæring i informasjonssikkerhet og personvern, og dokumenteres dette? | Art. 24 (1), 32 (1)(d) |
| 14 | Er det etablert et helhetlig styringssystem (internkontroll) for informasjonssikkerhet og personvern som dekker virksomhetens aktiviteter? | Art. 24 (1), 25 (1) |
| 15 | Er styringssystemet tilpasset virksomhetens størrelse, risiko, egenart og formål med behandlingen? | Art. 24 (1) |
| 16 | Er styringssystemet forankret hos ledelsen og gjort kjent i organisasjonen? | Art. 24 (1) |
| 17 | Gir øverste ledelse tilstrekkelige ressurser og rammer for gjennomføring av nødvendige aktiviteter? | Art. 24 (1) |
| 18 | Er styringssystemet dokumentert, oppdatert og arkivert slik at tidligere versjoner kan spores? | Art. 5 (2), 24 (1) |
| 19 | Er det vurdert om sensitiv informasjon skal fjernes eller skjermes før utlevering eller deling? | Art. 5 (1)(f) |
| 20 | Blir dokumentasjon av risiko, tiltak og kontroller oppdatert og tilgjengelig ved behov? | Art. 24 (1), 32 (1) |
| 21 | Har virksomheten definert mål og strategi for informasjonssikkerhet og personvern, og blir disse gjennomgått årlig? | Art. 24 (1) |
| 22 | Gjennomfører ledelsen jevnlig gjennomgang av styringssystemet og risikostatus, og dokumenteres resultatene? | Art. 24 (1), 32 (1)(d) |
| 23 | Har virksomheten etablert tekniske og organisatoriske tiltak for å ivareta konfidensialitet, integritet, tilgjengelighet og robusthet (CIA)? | Art. 32 (1)(b–d) |
| 24 | Blir det tatt hensyn til teknologisk utvikling, kostnader og behandlingens art ved valg av tiltak? | Art. 32 (1) |
| 25 | Er tiltakene forholdsmessige i forhold til risiko og tiltakets kostnad? | Art. 32 (1) |
| 26 | Ivaretas konfidensialitet gjennom tilgangsstyring, logging og taushetsplikt? | Art. 32 (1)(b), 5 (1)(f) |
| 27 | Ivaretas integritet ved at data holdes korrekte, komplette og beskyttes mot uautorisert endring eller sletting? | Art. 32 (1)(b–d) |
| 28 | Ivaretas tilgjengelighet og robusthet gjennom drift, gjenoppretting og redundans? | Art. 32 (1)(b–c) |
| 29 | Behandles brudd på konfidensialitet, integritet og tilgjengelighet som avvik, og meldes ved plikt? | Art. 33 (1), 34 (1) |
| 30 | Er det utarbeidet protokoll over behandlinger av personopplysninger (RoPA)? | Art. 30 (1) |

| | | |
|---|---|---|
| **31** | Har virksomheten oversikt over IKT-systemer og tjenester med betydning for informasjonssikkerheten? | Art. 30 (1), 32 (1) |
| **32** | Blir risikovurderinger gjennomført jevnlig, inkludert før nye behandlinger igangsettes? | Art. 35 (1) |
| **33** | Blir risikovurderinger og risikohåndtering dokumentert og kommunisert til ledelsen på riktig detaljnivå? | Art. 35 (7), 24 (1) |
| **34** | Er konsekvensvurdering for personvern (DPIA) gjennomført der høy risiko foreligger? | Art. 35 (3) |
| **35** | Foretas samråd med Datatilsynet der høy risiko ikke kan reduseres? | Art. 36 (1) |
| **36** | Testes og evalueres sikkerhetstiltak regelmessig for å sikre effektivitet og oppdatert risikobilde? | Art. 32 (1)(d) |
| **37** | Er alle involverte aktører kjent med rutiner for varsling av sikkerhetsbrudd og ansvar for oppfølging? | Art. 33 (1), 28 (3)(f) |

# Datadeling og datakonsumering

| Nr | Sjekkpunkt | Referanse |
|---|---|---|
| **1** | Har virksomheten kartlagt og dokumentert hvilken informasjon som opprettes og deles internt og eksternt? | Art. 30 (1) |
| **2** | Har virksomheten dokumentert prosess for datakatalogisering eller klassifisering som gir oversikt over hvilke data som kan deles – inkludert ansvar, publiseringsstatus og revisjonsrutine? | — |
| **3** | Er dataene beskrevet etter standarder som legger til rette for gjenbruk, interoperabilitet og felles begrepsbruk? | — |
| **4** | Har virksomheten hjemmel for å dele skjermede eller sensitive data, og er nødvendige sikkerhetstiltak på plass? | Art. 6 (1), 9 (2), 32 (1) |
| **5** | Har virksomheten inngått nødvendige databehandleravtaler og/eller datadelingsavtaler ved deling og behandling av data? | Art. 28 (3), 26 (1–2) |
| **6** | Har virksomheten oversikt over hvem som er mottakere og konsumenter av dataene? | Art. 30 (1)(d) |
| **7** | Er roller og ansvar mellom virksomheten, konsumenter og eventuelle tredjeparter klart avklart og dokumentert? | Art. 26, 28 |
| **8** | Ivaretas sikkerhetsprinsipper ved datadeling, herunder autentisering, autorisasjonskontroll og logging av tilganger? | Art. 32 (1)(b–d) |
| **9** | Er tekniske løsninger dokumentert og etablert for sikker publisering og deling av data, inkludert bruk av sikre grensesnitt og APIer? | Art. 32 (1) |
| **10** | Har virksomheten angitt om dataene utgjør en autoritativ kilde og publisert informasjon om dette? | — |
| **11** | Har virksomheten publisert datasett og API-er i Felles datakatalog? | — |
| **12** | Blir konfidensialitet, integritet og tilgjengelighet ivaretatt ved deling av data? | Art. 32 (1)(b–d) |
| **13** | Er det gjennomført vurderinger av sikkerhetsrisikoer ved deling av personopplysninger, spesielt for sensitive data? | Art. 35 (1) |
| **14** | Har virksomheten etablert tekniske løsninger for sikker utveksling av data og maskinlesbare grensesnitt? | Art. 32 (1) |
| **15** | Har virksomheten vurdert om data kan deles som åpne data dersom det ikke foreligger hindringer? | — |
| **16** | Benytter virksomheten fellesløsninger og felleskomponenter der det er mulig? | Art. 32 (1) |
| **17** | Har virksomheten etablert rutiner for drift, endringshåndtering og forvaltning av datadelingsløsninger? | Art. 32 (1)(d) |
| **18** | Gjennomføres risikovurderinger ved større endringer i samarbeid med konsument eller tilbyder? | Art. 32 (1)(d) |
| **19** | Bidrar alle parter i delingen til opprettholdelse og forbedring av informasjonssikkerheten? | Art. 32 (1)(d) |

| | | |
|---|---|---|
| **20** | Har virksomheten etablert rutiner for forvaltning og oppfølging av inngåtte delings- og behandlingsavtaler? | Art. 28 (3), 26 (1) |
| **21** | Har virksomheten vurdert om datadeling innebærer viderebehandling av personopplysninger, og hvilket behandlingsgrunnlag som gjelder? | Art. 6 (1), 5 (1)(b) |
| **22** | Har virksomheten vurdert om mottakerens formål er forenlig med innsamlingsformålet, og dokumentert vurderingen? | Art. 5 (1)(b), 6 (4) |
| **23** | Er det dokumentert at statistikk-, forsknings- eller arkivformål behandles i samsvar med art. 89 (1) (særlige garantier)? | Art. 5 (1)(b), 89 (1) |
| **24** | Er det avklart hvilket nivå i mottakende virksomhet som skal være behandlingsansvarlig for mottatte data? | Art. 24 (1), 26 (1) |
| **25** | Har virksomheten vurdert og dokumentert behandlingsgrunnlag hos konsument ved deling av personopplysninger? | Art. 6 (1), 9 (2) |
| **26** | Sikrer virksomheten at det ikke deles flere opplysninger enn nødvendig (dataminimering)? | Art. 5 (1)(c) |
| **27** | Er overføring av data til tredjeland vurdert og dokumentert, og brukes lovlig mekanisme eller garantier? | Art. 44–46 |
| **28** | Har virksomheten implementert innebygd personvern og beskyttelse av data i tekniske løsninger ved deling og mottak? | Art. 25 (1–2), 32 (1) |
| **29** | Har virksomheten gjennomført risikovurdering av mottak og viderebruk av data fra eksterne tilbydere? | Art. 32 (1), 35 (1) |
| **30** | Har virksomheten vurdert datakvalitet og oppdateringshyppighet for data mottatt fra tilbydere? | — |
| **31** | Har virksomheten etablert standardisert prosess for datakvalitetssjekk og dokumentasjon av kvalitet for formålet? | — |
| **32** | Har virksomheten vurdert om flere konsumenter kan samordne seg om felles mottak eller databehandling (tredjepart/segmentansvarlig)? | — |
| **33** | Er krav til omfang og hyppighet av datautvekslingen avklart mellom tilbyder og konsument? | — |
| **34** | Er roller og ansvar avklart med tilbyder, og er avtaler oppdatert ved endringer? | Art. 28 (3), 26 (1) |
| **35** | Har virksomheten vurdert om databehandlingen krever DPIA, og gjennomført denne ved høy risiko? | Art. 35 (1–3) |
| **36** | Har virksomheten etablert rutiner for sikker overføring og gjenoppretting ved feil eller databrudd? | Art. 32 (1)(b–d), 33 (1) |