



Oslo

Byrådsavdeling for finans

Praktiske retningslinjer for bruk av apper



Dette dokumentet skal gi ansatte og ledere i Oslo kommune praktiske retningslinjer og faglige råd for bruk av apper.

Praktiske retningslinjer for bruk av apper

Dette dokumentet skal gi ansatte og ledere i Oslo kommune praktiske retningslinjer og faglige råd for bruk av apper. Virksomheter i Oslo kommune kan ha ulike behov og ulikt utgangspunkt for å vurdere bruk av apper. Virksomhetene må selv gjøre de nødvendige vurderingene i forhold til denne behandlingen, for eksempel personvern vurderinger og risiko- og sårbarhetsanalyse (ROS). Virksomhetene må også sikre at de har behandlingsgrunnlag for all sin behandling av personopplysninger.

1. Om formålsbeskrivelse

Virksomhet må ha et spesifikt formål for behandlingen av personopplysninger. Det må sikres at behandlingen av personopplysninger i appen er nødvendig for å oppnå dette formålet.

Virksomheten må sikre at leverandøren ikke behandler personopplysninger til egne formål som markedsføring, analyse, statistikk, testing mv. uten at virksomheten er informert om dette. Dette er en av de største utfordringene ved bruk av apper. Virksomheten bør ha oversikt over at behandlingen av personopplysninger i appen er innenfor virksomhetens formål, og at leverandøren ikke behandler personopplysningene utover dette.

2. Personvern vurderinger

Det skal alltid gjennomføres personvern vurderinger før behandling av personopplysninger i apper starter. Dette innebærer alltid en innledende personvern vurdering (IP) og i tillegg enten personvern vurdering ved lav/middel risiko (PLM) eller personvern vurdering ved høy risiko (DPIA). Se [maler for personvurderinger og veileder](#).

3. Behandling av særlige kategorier av personopplysninger

Det er utfordrende å holde oversikt over hvilke personopplysninger som samles inn og om det samles inn særlige kategorier av personopplysninger som helseopplysninger ol. Dette kan spesielt være et problem når appene inneholder fritekstfelter. Særlige kategorier personopplysninger skal bare behandles når det er helt nødvendig og når eget behandlingsgrunnlag for dette er på plass. Unngå fritekstfelter hvis mulig, men hvis det benyttes bør det legges til hjelpetekst som sier hvilke personopplysninger som ikke skal registreres i appen.

4. Spesielle utfordringer knyttet til prinsipper for behandling av personopplysninger

I apper samles det ofte inn flere personopplysninger enn nødvendig eller personopplysninger som ikke er relevante, særlig ved bruk av fritekstfelter. Virksomheten bør gjøre konkrete vurderinger av hvilke personopplysninger som er nødvendige for å oppnå formålet, og om det er mulig å begrense funksjonalitet i appen (dataminimering).

I apper skjer det ofte at personopplysninger blir lagret lenger enn de skal eller at tilleggstjenester som posisjonstjenester ol. utilsiktet samler inn og lagrer personopplysninger. Det må sikres at det er gode rutiner for sletting av personopplysninger og at dere har kontroll på at slettingen blir gjennomført (lagringsbegrensning).

Ansvarsforholdene kan være spesielt utfordrende for apper, og dette må avklares før appen tas i bruk. Virksomheten må blant annet avklare hvem og hvordan de registrertes rettigheter skal ivaretas, for eksempel som en del av databehandleravtalen (ansvarlighet).

5. Spesielle utfordringer knyttet til den registrertes rettigheter

Den registrerte skal få lett tilgjengelig informasjon som er tilpasset egen målgruppe. Ofte skjer det kontinuerlige oppdateringer i appen som påvirker den registrertes personvern, da bør også informasjonen til den registrerte oppdateres (rett til informasjon).

Innsyn kan være utfordrende fordi virksomheten ikke selv har tilgang til personopplysningene som behandles i appen. Det bør avklares på forhånd hvordan innsyn skal håndteres (rett til innsyn).

6. Dokumentasjon

Virksomhetene må ha følgende dokumentasjon:

- ▶ Personvern vurderinger og ROS
- ▶ Databehandleravtaler (hvis relevant)
- ▶ Involvering av Personvernombudet dersom det er snakk om DPIA, se mal for personvern vurdering ved høy risiko (DPIA)
- ▶ Ledelsesinvolvering og forankring
- ▶ Registrering i virksomhetens behandlingsoversikt

7. Overføring til utlandet

Dersom det viser seg at personopplysninger overføres til utlandet i forbindelse med bruk av apper, må det sikres følgende:

- ▶ Det finnes nødvendig overføringsgrunnlag
- ▶ Det finnes ytterligere tiltak dersom det er snakk om overføring til tredjeland (land utenfor EU/EØS)
- ▶ Ledelsesinvolvering og forankring

8. Andre forhold

Det er ofte utfordrende å oppnå kontakt med og innhente nødvendig informasjon om hvordan app-leverandøren og deres underleverandører behandler personopplysningene. Dette er en risiko som virksomhetene bør være oppmerksomme på og håndtere så tidlig som mulig. For vide eller ugjenkallelige lisenser til brukernes innhold som kan gis eller selges videre bør unngås.

Relevante kilder og dokumenter:

- ▶ EDPB: Guidelines on the protection of personal data processed by mobile applications provided by European Union institutions
- ▶ Datatilsynet: Elementer for å sikre tillitsfull og ansvarlig bruk av apper (del av Veiledning om apper til støtte for bekjempelse av Covid-19-pandemien)