Visma Compliance

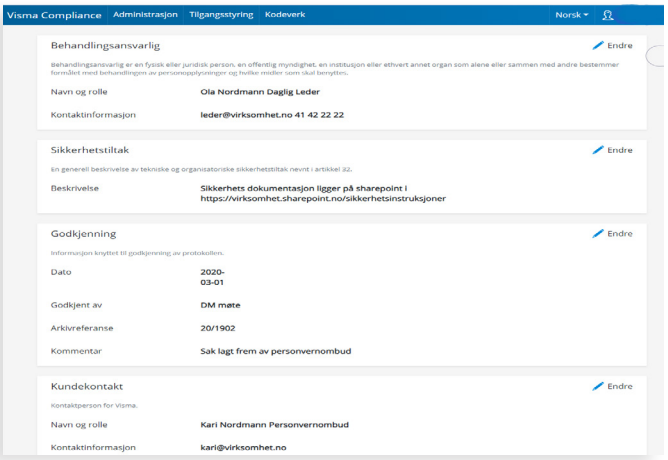
Visma Compliance er en online SaaS-tjeneste som på en sikker måte lar virksomheter føre protokoll i henhold til artikkel 30 i Lov om behandling av personopplysninger (personopplysningsloven). Løsningen er utviklet i tett samarbeid med Visma sine kunder og utgjør en solid plattform for effektiv ledelse og styring av virksomhetens personvern.

Personopplysninger

I artikkel 30 i personopplysningsloven står det at behandlingsansvarlige skal føre protokoll over behandlingsaktiviteter som utføres under deres ansvar. Protokollen skal blant annet inneholde informasjon om formål med behandlingen, hvilke kategorier av personopplysninger den inneholder, og hvem personopplysningene deles med. Protokollen skal på anmodning kunne gjøres tilgjengelig for tilsynsmyndigheten.

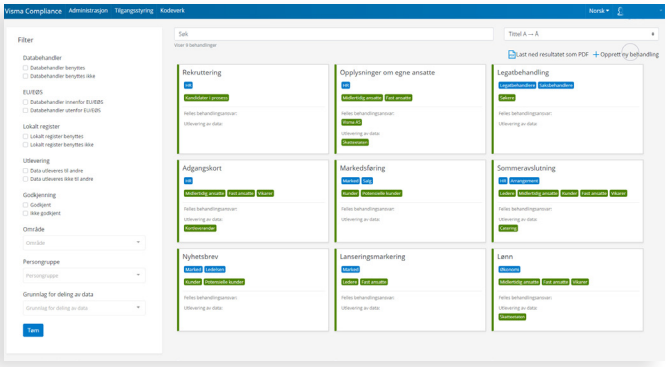
Produktet

I Visma Compliance kan virksomheter som behandler personopplysninger registrere og holde oversikt over sine behandlingsaktiviteter. Søk- og filtreringsfunksjonen gjør det enkelt å finne frem til behandlinger knyttet til for eksempel en gitt persongruppe, avdeling eller IT-system. I tillegg til å kunne registrere den lovpålagte informasjonen om hver enkelt behandlingsaktivitet, kan virksomheten registrere informasjon knyttet til protokollen i sin helhet.



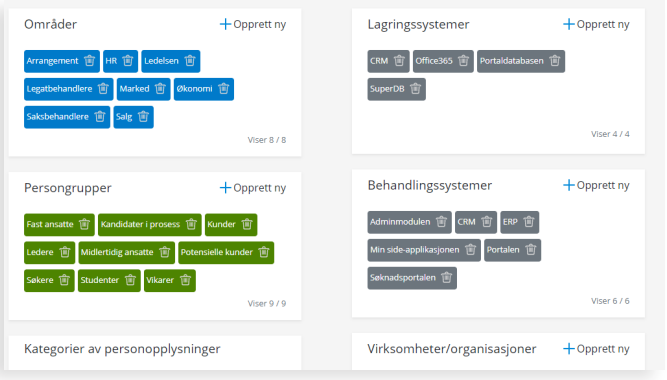
Behandlingsaktiviteter

Ved registrering av en ny behandlingsaktivitet, blir brukeren veiledet gjennom et skjema med felter for utfylling. Her registreres informasjon om behandlingsgrunnlag, hvilke typer personopplysninger det er snakk om, hvor de er lagret, når de skal slettes osv. Det er informasjon som hver behandlingsansvarlig ifølge artikkel 30 i personopplysningsloven er pliktig til å inkludere i protokollen. Personopplysningsloven skiller mellom behandling av generelle personopplysninger, særlige kategorier av personopplysninger (artikkel 9), og personopplysninger om straffedommer og lovovertredelser (artikkel 10). Visma Compliance gjenspeiler det. Dersom det er en eller flere databehandlere involvert (artikkel 28), eller et felles behandlingsansvar (artikkel 26), må det registreres i protokollen. Der det er aktuelt, kan brukeren laste opp relevante filer. Det gjør at virksomheten kan samle både databehandleravtaler og samtykkeskjemaer i løsningen hvis det er ønskelig.



Kodeverk

For å øke datakvaliteten, samt forenkle registrering av nye behandlingsaktiviteter, velger den enkelte virksomheten hvilke personopplysningskategorier, IT-systemer og lovhjemler som vil være aktuelle for sin protokoll. Disse inngår i et kodeverk som virksomheten selv administrerer gjennom en rettighetsstyrt administrasjonmodul.



Rapportering og risikostyring

Løsningen støtter både nedlastning av protokollen i sin helhet, og nedlastning av utvalgte behandlingsaktiviteter. I forbindelse med godkjenning av protokollen på ledelsesnivå, er det nyttig å kunne eksportere en komplett samling av virksomhetens behandlingsaktiviteter. Ved tilsyn vil det kunne være aktuelt å hente ut et sett med etterspurte behandlingsaktiviteter. For å bestemme hvilke behandlingsaktiviteter som skal inkluderes i rapporten, benyttes søk- og filtreringsfunksjonaliteten i løsningen. Rapporten er i formatet PDF.
Gjennom kategorisering vil det fremkomme veldig tydelig hvilken risiko organisasjonen har i håndtering av persondata. Dette er viktig både som styringsinformasjon og som verktøy ved hendelser som for eksempel angrep på systemer og infrastruktur.

Rettighetsstyring og integrasjon med virksomhetens AD

God arbeidsflyt sikres best når verktøyene er lett tilgjengelige. Visma Compliance gjøres tilgjengelig med single sign-on (SSO) for virksomheten. Løsningen integreres med virksomhetens Azure Active Directory (Azure AD), og lar brukerne logge inn i løsningen med sitt eksisterende brukernavn og passord. Det gir også Azure AD-administratorer hos virksomheten mulighet til å styre hvem som skal ha tilgang når, og til hvilke roller i stystemet. Tilgang kan styres på individ- eller gruppenivå. Det er også mulig å sette opp regler for når og fra hvilke lokasjoner brukere skal kunne logge seg inn. Multifaktorautentisering (MFA) kan aktiveres dersom det er ønskelig.

Sikkerhet

Visma Compliance er bygget med moderne skyarkitektur hvor fokuset har vært sikkerhet i alle ledd. Flere deler av Visma er ISO 27001 sertifisert, og drift og utvikling av Compliance følger sertifiserte arbeidsprosesser og standarder. Forvaltning og drift baserer seg også på ISO 20000. All infrastruktur og leveranser av disse følger strenge sertifiseringer. Løsningen kjører i Azure Norge, som er de norske datasentrene til Microsoft. Data lagres og behandles innenfor EU/EØS med bransjens beste sikkerhet.

Ytre sikring av API og nettside

Visma Compliance er eksponert til sluttbrukere med en nettside og tilhørende API. Grensesnittene er sikret med en distribuert bransjeledende brannmur. Brannmuren sikrer løsningen mot de til enhver tid gjeldende OWASP-truslene og andre typer angrep. Brannmuren er også koblet sammen med lastbalanserer som vil sende brukerne til en online instans. Det gjør det mulig å holde løsningen oppe ved stor last og under tjenestenektsangrep. Både API og nettside har egne sikkerhetsmekanismer i tillegg til brannmuren, og vil i seg selv være motstandsdyktige mot angrep.

Adskilte Virksomhetsdata

Data lagres i en distribuert dokumentbase. Hver virksomhet har sin egen container med data. Denne er det kun virksomheten selv som får lese fra, og skrive data til. Det er i denne lagringsmekanismen alle brukere, kodeverk og oppføringer blir lagret. Informasjon om virksomheten, som tenant id, navn og kontaktperson, ligger lagret i en felles container. Løsningen leser fra denne for å finne riktig database, samt at Visma har behov for å lese kontaktinformasjonen oppgitt av virksomheten selv.

Sikkerhetskopier

Det tas kontinuerlig sikkerhetskopier av data og oppsett. Det gjør at data kan gjenopprettes ved utfall. Det blir også ført endringslogg på alle data.

Personopplysninger

Løsningen lagrer og behandler visningsnavn, epostadresse og object id fra virksomhetens Azure AD. Disse opplysningene lagres og behandles i Norge, innenfor EU/EØS. Alle data blir slettet ved endt kundeforhold, og opplysningene benyttes utelukkende til virksomhetens egen bruk i løsningen. Herunder visning i skjermbilder, rapporter og eventuell epostutsendelse. Enkeltbrukere kan slettes fra løsningen av virksomheten selv. Spor av brukeren vil bli liggende der det er nødvendig for revisjon. Behandling av personopplysningene er i henhold til gjeldende GDPR-regelverk, og omfattes av databehandleroppgave.
Virksomheten kan oppgi navn og kontaktinformasjon til enkeltpersoner i protokollen, noe som anses som personopplysninger. Disse opplysningene blir behandlet som personopplysninger uavhengig av hva som oppgis. Virksomheten er selv ansvarlig for ajourføring av disse dataene.

Begreper

- **Azure Active Directory** – Skyvarianten av Microsoft sin brukerkatalog. Alle med Microsoft Office 365 benytter denne i kulissene.
- **Behandlinsaktivitet** – Virksomheter som behandler personopplysninger, skal føre en protokoll over hvilke personopplysninger som behandles under deres ansvar. Hvert innslag i protokollen, kalles en behandlingsaktivitet.
- **Behandlingsansvarlig** – Fysisk eller juridisk person som bestemmer formålet med behandlingen av personopplysninger, samt hvilke midler som skal benyttes.
- **Kodeverk** – Et sett med statiske verdier som kan benyttes ved utfylling av protokollen.

VISMA