Når man bruker Kostholdsplanleggeren som privatperson, er det Helsedirektoratet som er ansvarlig for å behandle personopplysninger og som skal behandle disse i samsvar med personvernerklæringen for Kostholdsplanleggeren og gjeldende regelverk. Når man bruker Kostholdsplanleggeren som elev, student eller som ansatt i en virksomhet er det skole/utdanningsinstitusjon/arbeidsplass som er behandlingsansvarlig for personopplysningene. Helsedirektoratet skal da behandle opplysningene i henhold til en databehandleravtale som er inngått mellom Helsedirektoratet og skole/utdanningsinstitusjon/arbeidsplass. Skoler, utdanningsinstitusjoner og andre virksomheter velger om de vil ta Kostholdsplanleggeren i bruk for egne elever, studenter og ansatte. Virksomheter som tidligere har inngått avtale med Mattilsynet må inngå ny databehandleravtale med Helsedirektoratet.

Databehandleravtale

mellom

[Brukeren av Kostholdsplanleggeren]

(heretter kalt "Behandlingsansvarlig")

og

Helsedirektoratet

(heretter kalt "Databehandler")

Om Databehandlers (Helsedirektoratets) behandling av personopplysninger på vegne av Behandlingsansvarlig

Bakgrunn og formål

Behandlingsansvarlig ønsker å ta i bruk tjenesten Kostholdsplanleggeren ("**Tjenesten**") som leveres av Databehandler.

I forbindelse med Tjenesten vil Databehandler kunne behandle Personopplysninger i henhold til Lov om behandling av personopplysninger av 15.juni 2018 nr. 38 som iverksetter Europaparlaments- og rådsforordning (EU) 2016/679 av 27.april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger (General Data Protection Regulation)

(heretter omtalt som "personvernforordningen"). Denne avtalen regulerer slik behandling av Personopplysninger på vegne av Behandlingsansvarlig som ledd i bruken av Tjenesten.

Tjenesten er et gratis kostberegningsprogram der enkeltpersoner kan beregne summen av næringsinnhold i registrerte matvarer og sammenlikne med norske anbefalinger for inntak av energi og næringsstoffer.

Kostholdsplanleggeren kan brukes av alle som vil vite hva maten inneholder og som vil planlegge eget kosthold.

Kostholdsplanleggeren brukes i faget "Mat og helse" i grunnskolen, undervisning for helsefag på videregående og ernærings- og helsefag i høyere utdanning, i kostholdsopplæring og ernæringsveiledning.

Formålet med Databehandlerens behandling av personopplysninger på vegne av Behandlingsansvarlig er å levere og administrere Tjenesten ved å vise, beregne og sammenlikne næringsinnhold i matvarer, retter, måltider og dags- og ukeinntak. Personopplysninger som behandles som databehandler vil være ID for bruker og brukerens menyer.

Pålogging i tjenesten skjer gjennom påloggingstjenestene Feide og ID-porten. Når brukeren logger seg inn gjennom autentiseringsleverandører (Feide eller ID-porten), får Databehandler (Helsedirektoratet) oversendt en unik tallkode for brukeren fra Feide eller ID-porten. Direktoratet kan ikke selv spore denne tallkoden tilbake til brukerens navn eller e-post.

Behandling av personopplysninger i forbindelse med påloggingen via Feide reguleres i særskilt avtale med Feide.

Denne databehandleravtalen ("**Databehandleravtalen**") oppfyller kravet om databehandleravtale etter personopplysningsloven. Databehandleravtalen angir Databehandlers rådighet over Personopplysninger som behandles på vegne av Behandlingsansvarlig, og angir Databehandlers ansvar for informasjonssikkerhet etter personopplysningsloven.

Definisjoner

I denne databehandleravtalen skal begrepene nedenfor ha den betydning som til enhver tid følger av personvernforordningen artikkel 4:

1) «personopplysninger» er 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,

2)«behandling» er 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,

3) «begrensning av behandling» er merking av lagrede personopplysninger med det som mål å begrense behandlingen av disse i framtiden,

4) «profilering» er enhver form for automatisert behandling av personopplysninger som innebærer å bruke personopplysninger for å vurdere visse personlige aspekter knyttet til en fysisk person, særlig for å analysere eller forutsi aspekter som gjelder nevnte fysiske persons arbeidsprestasjoner, økonomiske situasjon, helse, personlige preferanser, interesser, pålitelighet, atferd, plassering eller bevegelser»

5) «pseudonymisering» behandling av personopplysninger på en slik måte at personopplysningene ikke lenger kan knyttes til en bestemt registrert uten bruk av tilleggsopplysninger, forutsatt at nevnte tilleggsopplysninger lagres atskilt og omfattes av tekniske og organisatoriske tiltak som sikrer at personopplysningene ikke kan knyttes til en identifisert eller identifiserbar fysisk person,

6) «register» er enhver strukturert samling av personopplysninger som er tilgjengelig etter særlige kriterier, enten samlingen er plassert sentralt, er desentralisert eller spredt på et funksjonelt eller geografisk grunnlag,

7) «behandlingsansvarlig» er en fysisk eller juridisk person, en offentlig myndighet, en institusjon eller ethvert annet organ som alene eller sammen med andre bestemmer formålet med behandlingen av personopplysninger og hvilke midler som skal benyttes; når formålet med og midlene for behandlingen er fastsatt i unionsretten eller i medlemsstatenes nasjonale rett, kan den behandlingsansvarlige, eller de særlige kriteriene for utpeking av vedkommende, fastsettes i unionsretten eller i medlemsstatenes nasjonale rett,

8) «databehandler» er en fysisk eller juridisk person, offentlig myndighet, institusjon eller ethvert annet organ som behandler personopplysninger på vegne av den behandlingsansvarlige.

Beskrivelse av behandlingen

Denne Databehandleravtalen gjelder all behandling av Personopplysninger som Databehandler utfører på vegne av den Behandlingsansvarlige i forbindelse med Tjenesten. Databehandleren kan bare behandle de kategorier av Personopplysninger som er forutsatt i Tjenesten og i den grad det er nødvendig for å levere og administrere Tjenesten.

Helsedirektoratet behandler følgende personopplysninger i løsningen:

- bruker-ID utstedt av Feide,
- Brukerens ukemenyer
- eventuelt informasjon som brukeren legger inn i fritekstfelt.

Det er lagt inn veiledningstekst i løsningen som oppfordrer bruker til å ikke legge inn særlig kategori av personopplysninger i løsningen.

Bruker-ID Helsedirektoratet mottar fra Feide er ID-generert av Feide. Helsedirektoratet behandler derfor ikke fødselsnummer om brukeren.

Databehandlers plikter

Etterlevelse av krav i lov og forskrift

I avtaleperioden skal Databehandler overholde alle relevante bestemmelser i personvernforordningen.

Databehandler skal ikke ved handling eller unnlatelse sette den Behandlingsansvarlige i en situasjon der Behandlingsansvarlig misligholder en eller flere bestemmelser i personvernforordningen.

Databehandler skal samarbeide med og yte bistand til den Behandlingsansvarlige for å sikre at Behandlingsansvarlig overholder sine forpliktelser i henhold til personopplysningsregelverket.

Behandlingsansvarlig har, med mindre annet er avtalt eller følger av lov, rett til tilgang til og innsyn i personopplysningene som behandles på vegne av Behandlingsansvarlig og systemene som benyttes til dette formål.

Databehandleren skal på forespørsel bistå Behandlingsansvarlig så langt det er mulig med oppfyllelse av de registrertes rettigheter etter personvernforordningen kapittel III gjennom egnede tekniske eller organisatoriske tiltak. Registrertes rettigheter til innsyn, endring og retting av informasjon er nærmere omtalt i personvernerklæringen.

Databehandler skal overholde de til enhver tid gjeldende instrukser og rutiner for behandling av Personopplysninger som Behandlingsansvarlig har vedtatt.

Begrensninger vedrørende bruk

Databehandler skal ikke behandle Personopplysninger utover det som kreves for å levere og administrere Tjenesten til Behandlingsansvarlig i henhold til vilkår for bruk av Tjenesten.

Databehandler skal påse at Personopplysninger ikke gis til utenforstående med mindre Behandlingsansvarlig har pålagt slik utlevering eller Databehandler er forpliktet til dette i medhold av lov.

Databehandler skal ikke ha rettigheter til eller eierskap over Personopplysninger som Databehandler får tilgang til som ledd i leveranse av Tjenesten.

Dersom bruker ikke er aktiv på 24 måneder, så slettes alt som er registrert på bruker, det vil si ukemenyer, matretter, matvarer og næringsstoffer.

Informasjonssikkerhet

Databehandler skal ved hjelp av planlagte, systematiske organisasjonsmessige og tekniske tiltak sikre tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet og tilgjengelighet i forbindelse med behandling av Personopplysninger i henhold til Personvernforordningen artikkel 28 pkt.1., samt Personvernforordningen artikkel 32 pkt. 1. til 4.

Dokumentasjon av sikkerhetstiltak

For å oppnå tilfredsstillende informasjonssikkerhet skal Databehandler, på forespørsel fra den Behandlingsansvarlige, fremlegge dokumentasjon for datasystemer og sikkerhetstiltak. Rutiner for bruk

av informasjonssystemet og annen informasjon med betydning for informasjonssikkerheten, skal dokumenteres.

Avvik

Enhver bruk av informasjonssystemet som er i strid med Databehandlers fastlagte rutiner, den Behandlingsansvarliges instrukser eller Personvernforordningen, samt ethvert sikkerhetsbrudd, skal behandles som et avvik.

Databehandler skal ha på plass rutiner og systematiske tiltak for oppfølging av avvik, herunder tiltak for gjenoppretting av normal tilstand, fjerning av årsaken til avviket og hindre gjentakelse.

Databehandler skal rapportere avvik til den Behandlingsansvarlige uten ugrunnet opphold. Rapporten skal omfatte informasjon om hvilke tiltak Databehandler har gjort for å gjenopprette normal tilstand, fjerne årsaken til avviket og hindre gjentakelse. Databehandler skal også gi Behandlingsansvarlig alle nødvendige opplysninger for å kunne besvare spørsmål fra datatilsynsmyndigheter og etterleve eventuelle krav om varsling til Datatilsynet og berørte registrerte.

Sikkerhetsrevisjon

Databehandler er innforstått med at den Behandlingsansvarlige regelmessig og minst en gang årlig kan gjennomføre sikkerhetsrevisjoner av informasjonssystemet og tilhørende fasiliteter som benyttes av Databehandler for behandling av Personopplysninger på vegne den Behandlingsansvarlige.

Bruk av underleverandører

Databehandler benytter Norsk Helsenett som underleverandør. Norsk Helsenett benytter igjen Microsoft som underleverandør. Databehandler er ansvarlig for arbeid som utføres av underleverandør, og skal påse at underleverandøren påtar seg ansvar i samsvar med forpliktelsene som angitt i denne Databehandleravtalen. Ved ønske om endring i underleverandør skal den dataansvarlige underrettes i god tid, slik at det gis mulighet til å motsette seg endringen.

Overføring til utlandet

Bruk av underleverandører som overfører personopplysninger til land utenfor EU/EØS (tredjeland) skal avtales skriftlig med Dataansvarlig på forhånd. Ved overføring av personopplysninger til land utenfor EU/EØS (tredjeland) skal Databehandler benytte godkjente EU-overføringsmekanismer.

Dataene i Kostholdsplanleggeren behandles på servere i EU og lagres i database i skyløsning i Norge fra Microsoft. Ved behov for tilgang til personopplysninger ved support fra Microsoftpersonell fra andre land, vil en overføring av opplysninger kun skje der det er strengt nødvendig og etter inngått Standard Contractual Clauses. Databehandler vil ikke overføre direkte identifiserbare er personopplysninger utenfor EØS-området ved slik eventuelt behov for support.

Konfidensialitet

Databehandleren påtar seg å ivareta taushet om enhver opplysning som behandles på vegne av den Behandlingsansvarlige i henhold til vilkår for bruk av Tjenesten eller denne databehandleravtalen. Taushetsplikten omfatter også annen informasjon av betydning for informasjonssikkerheten. Taushetsplikten skal også gjelde etter utløpet av denne Databehandleravtalen.

Databehandler skal påse at godkjente underleverandører som behandler Personopplysninger på vegne av den Behandlingsansvarlige i henhold til pkt. 4.8 er kjent med denne Databehandleravtalen og sørge for at de er underlagt vilkårene i denne, herunder kravene til konfidensialitet.

Kostholdsplanleggeren har tilgangsstyring slik at bare autorisert personell hos Databehandler og underleverandører har tilgang.

Varighet og opphør av Databehandleravtalen

Denne Databehandleravtalen gjelder fra den dato begge parter har signert Databehandleravtalen og frem til Behandlingsansvarlig slutter å bruke Tjenesten, bortsett fra eventuelle vilkår som i henhold til denne Databehandleravtalen eller vilkår for bruk av Tjenesten skal fortsette å ha virkning etter opphør.

Databehandler vil da slette opplysningene som behandles på vegne av den Behandlingsansvarlige.

Databehandleren har ingen rett til å beholde kopier av opplysninger i noe som helst format.

Den Behandlingsansvarlige skal motta en skriftlig erklæring fra Databehandleren om at samtlige opplysninger enten er tilbakelevert eller slettet i samsvar med eventuell instruks fra den Behandlingsansvarlige, og at Databehandleren ikke har beholdt noen kopi, utskrift eller annen fremstilling av opplysninger på noe som helst medium.

Ved brudd på Databehandleravtalen og/eller gjeldende personvernregler, kan Behandlingsansvarlig og aktuelle tilsynsmyndigheter pålegge Databehandler å stoppe hele eller deler av behandlingen av opplysningene med øyeblikkelig virkning.

Lovvalg og tvisteløsning

Partenes rettigheter og plikter etter denne Databehandleravtalen bestemmes i sin helhet etter norsk rett.

Oslo tingrett vedtas som eksklusivt verneting.

Partene kan som alternativ til domstolsbehandling avtale at tvisten avgjøres med endelig virkning ved voldgift.

Signatur

Databehandleravtalen er utstedt i 2 – (to) – eksemplarer, hvorav partene beholder hvert sitt.

Brukeren av Kostholdsplanleggeren	[**Helsedirektoratet**]
Dato: …….	Dato: ……
Signatur: ……	Signatur: …….
Navn: ……	Navn: ……..
Tittel: ……	Tittel: ……..