

## **1. Bakgrunnen for denne personvernerklæringen**

- 1.1 Personvernerklæringen beskriver hvordan Wolters Kluwer Norge AS (Wolters Kluwer) behandler personopplysninger i forbindelse med at vi yter support til våre abonnementskunder. Kunden er da behandlingsansvarlig og Wolters Kluwer er databehandler.
- 1.2 Databehandlerens behandling av personopplysninger skjer for å oppfylle abonnementsavtalen, hvor fri support inngår. Hjemmel til å behandle personopplysninger er således at behandlingen er «nødvendig for å oppfylle en avtale som den registrerte er part i.» (personvernforordningen art. 6 litra b)
- 1.3 Denne personvernerklæringen frigjør ikke databehandleren for plikter, som etter personvernforordningen eller enhver annen lovgivning direkte er pålagt databehandleren.

## **2. Behandlingen kan omfatte følgende typer personopplysninger og kategorier registrerte**

- 2.1 Navn, adresse, e-postadresse, telefonnummer, fødselsdato/ fødselsnummer, regnskapsopplysninger til bruk for årsregnskaper, bilag til skattemelding og lignende økonomiske oppgjør for den behandlingsansvarliges kunder, samt opplysninger om den behandlingsansvarliges kunders nøkkelpersonell og ledelse, herunder navn, adresse, e-postadresse, telefonnummer og fødselsdato/ fødselsnummer.
- 2.2 Personer, som er eller har vært kunder hos den behandlingsansvarlige og personer som er eller har vært ansatt hos den behandlingsansvarlige.

## **3. Den behandlingsansvarliges plikter og rettigheter**

- 3.1 Den behandlingsansvarlige har overfor omverdenen (herunder den registrerte) som utgangspunkt ansvaret for at behandlingen av personopplysninger skjer innenfor rammene av personvernforordningen og personopplysningsloven.
- 3.2 Den behandlingsansvarlige har derfor både rett og plikt til å treffe beslutninger om til hvilke formål og med hvilke hjelpemidler behandlingen foretas.
- 3.3 Den behandlingsansvarlige er blant annet ansvarlig for, at det foreligger hjemmel til den behandling som databehandleren instrueres i å foreta.

## **4. Databehandleren handler etter instruks**

- 4.1 Databehandleren skal kun behandle personopplysninger etter dokumentert instruks fra den behandlingsansvarlige, medmindre det kreves i henhold til EU/ EØS-retten eller medlemsstatenes nasjonale rett, som databehandleren er underlagt. I så fall underretter databehandleren den behandlingsansvarlige om dette rettslige kravet innen behandling, medmindre den gjeldende rett forbyr en slik underretning av hensyn til viktige allmenne interesser, jf. art 28, nr. 3, litra a. Abonnementsavtalen mellom behandlingsansvarlig og databehandler anses som en slik instruks.
- 4.2 Databehandleren underretter omgående den behandlingsansvarlige, hvis en instruks etter databehandlerens mening er i strid med personvernforordning en eller databeskyttelsesbestemmelser i annen EU/EØS-rett eller medlemsstatenes nasjonale rett.

## 5. Fortrolighet

- 5.1 Databehandleren skal sikre at kun autoriserte personer har adgang til de personopplysninger som behandles på vegne av den behandlingsansvarlige. Adgangen til opplysningene skal derfor straks stenges hvis autorisasjonen fratas eller utløper.
- 5.2 Det skal bare autoriseres personer for hvem det er nødvendig å ha tilgang til personopplysningene for å kunne oppfylle databehandlerens forpliktelser overfor den behandlingsansvarlige.
- 5.3 Databehandleren skal sikre at de personene som er autorisert til å behandle personopplysninger på vegne av den behandlingsansvarlige, har forpliktet seg til fortrolighet eller er underlagt lovbestemt taushetsplikt.
- 5.4 Databehandleren skal etter anmodning fra den behandlingsansvarlige kunne dokumentere at de relevante medarbeidere er underlagt ovennevnte forpliktelser.

## 6. Behandlingsikkerhet

- 6.1 Databehandleren skal iverksette de tekniske og organisatoriske tiltak som kreves for å oppnå et sikkerhetsnivå som er egnet i forhold til risikoen, jf personverforordningens artikkel 32. Det skal bl.a. tas hensyn til implementeringsomkostningene, den aktuelle behandlings karakter, omfang, sammenheng og formål.
- 6.2 Ovenstående forpliktelse innebærer at databehandleren skal foreta en risikovurdering og gjennomføre tiltak for å minimere identifiserte risikoer. Det kan herunder bl.a., alt etter hva som er relevant, dreie seg om følgende foranstaltninger:
  - a. Pseudonymisering og kryptering av personopplysninger
  - b. Evne til å sikre vedvarende fortrolighet, integritet, tilgjengelighet og robusthet av behandlingssystemer og tjenester
  - c. Evne til rettidig å gjenopprette tilgjengeligheten av og adgangen til personopplysninger dersom det oppstår fysisk eller teknisk brudd på adgangen
  - d. En prosedyre for regelmessig prøvning, vurdering og evaluering av effektiviteten av de tekniske og organisatoriske foranstaltninger til sikring av personopplysninger
- 6.3 Personopplysninger som den behandlingsansvarlige stiller til rådighet for databehandleren til bruk for en supportoppgave, slettes fortløpende og senest ultimo den måned, hvor supportoppgaven har vært avsluttet i 3 måneder.

## 7. Bruk av underdatabehandlere

- 7.1 Databehandleren skal oppfylle de betingelser, som er omhandlet i personvernforordningens artikkel 28, pkt. 2 og 4, for å gjøre bruk av en annen databehandler (underdatabehandler).
- 7.2 Databehandleren skal ikke gjøre bruk av andre underdatabehandlere en de som fremgår av nedenstående tabell uten forutgående spesifikk eller generell skriftlig godkjenning fra den behandlingsansvarlige.
- 7.3 Ved generell skriftlig godkjenning skal databehandleren underrette den behandlingsansvarlige om eventuelle planlagte endringer vedrørende tilføyelse eller erstatning av underdatabehandlere og derved gi den behandlingsansvarlige mulighet for å gjøre innsigelse mot slike endringer.
- 7.4 Databehandleren skal pålegge underdatabehandlerne de samme forpliktelser til vern av personopplysninger som de som er fastsatt i denne personvernerklæringen, gjennom en databehandleravtale eller annet rettslig dokument i henhold til EU/EØS-retten eller medlemsstatenes

nasjonale rett, hvor det stilles de nødvendige garantier for at underdatabehandleren vil gjennomføre de passende tekniske og organisatoriske tiltak på en slik måte, at behandlingen oppfyller kravene i personvernforordningen.

7.5 Databehandleren er ansvarlig for, igjennom inngåelsen av en underdatabehandleravtale å pålegge en eventuell underdatabehandler minst de forpliktelser som databehandleren selv er underlagt etter personvernreglene og denne personvernerklæringen.

Underdatabehandleravtalen med eventuelle senere endringer sendes, etter den behandlingsansvarliges anmodning, i kopi til den behandlingsansvarlige, som med dette har mulighet for å sikre seg at der er inngått en gyldig avtale mellom databehandleren og underdatabehandleren. Eventuelle kommersielle vilkår, eksempelvis priser, som ikke påvirker sikkerhetsnivået i underdatabehandleravtalen, skal ikke sendes til den behandlingsansvarlige.

7.6 Dersom underdatabehandler ikke oppfyller sine forpliktelser til vern av personopplysninger, skal databehandler overfor behandlingsansvarlig ha fullt ansvar for at underdatabehandler oppfyller sine forpliktelser.

I forbindelse med supporten benyttes følgende underdatabehandlere:

Navn	Adresse	Beskrivelse av behandling
Penneo ApS	Enghavevej 40, 4. sal 1674 København V Danmark	Digital signatur
Multisoft	Brunkelbergstorg 5, 11151 Stockholm, Sverige	Utvikling og support av lisenssystem

## 8. Overføring av personopplysninger til tredjestat eller internasjonale organisasjoner

8.1 Databehandleren skal kun behandle personopplysninger etter dokumentert instruks fra den behandlingsansvarlige dersom det skal overføres personopplysninger til tredjestat (stater utenfor EU/EØS- området) eller internasjonale organisasjoner, medmindre det kreves i henhold til EU/EØS-retten eller medlemsstatenes nasjonale rett, som databehandleren er underlagt. I så fall underretter databehandleren den behandlingsansvarlige om det rettslige kravet innen behandling, medmindre den aktuelle rett forbyr slik underretning av hensyn til viktige allmenne interesser, jf. art 28, pkt. 3, litra a.

8.2 Uten den behandlingsansvarliges instruks eller godkjenning kan databehandleren, innenfor rammene av personvernerklæringen, derfor bl.a. ikke;

- videregi personopplysningene til en dataansvarlig i en tredjestat eller i en internasjonal organisasjon,
- overlate behandlingen av personopplysninger til en underdatabehandler i en tredjestat,
- Behandle personopplysningene i en annen av databehandlerens avdelinger, som er plassert i en tredjestat.

## 9. Bistand til den behandlingsansvarlige

9.1 Databehandleren bistår, hensyntatt behandlingens karakter, så vidt mulig den behandlingsansvarlige, ved hjelp av passende tekniske og organisatoriske tiltak, med oppfyllelse av den behandlingsansvarliges plikt til å besvare anmodninger om utøvelsen av de registrertes rettigheter som fastlagt i personvernforordningens kapittel 3.

Dette innebærer at databehandleren så vidt mulig skal bistå den behandlingsansvarlige i forbindelse med at den behandlingsansvarlige skal sikre overholdelsen av:

- a. opplysningsplikten ved innsamling av personopplysninger hos den registrerte
- b. opplysningsplikten, hvis personopplysninger ikke er innsamlet hos den registrerte
- c. den registrertes innsynsrett
- d. retten til korrigerings
- e. retten til sletting («retten til å bli glemt»)
- f. retten til begrensning av behandling
- g. underretningsplikt i forbindelse med korrigerings eller sletting av personopplysninger eller begrensning av behandling
- h. retten til dataportabilitet
- i. retten til innsigelse
- j. retten til å gjøre innsigelse mot resultatet av automatiske individuelle avgjørelser, herunder profilering

9.2 Databehandleren bistår den behandlingsansvarlige med å sikre oppfyllelse av den behandlingsansvarliges plikter i samsvar med personvernforordningens artikkel 32-36, hensynstatt behandlingens karakter og de opplysninger som er tilgjengelige for databehandleren, jf. art 28, nr. 3, litra f.

Dette innebærer at databehandleren skal bistå den behandlingsansvarlige i forbindelse med at den behandlingsansvarlige skal sikre overholdelsen av:

- a. plikten til å gjennomføre passende tekniske og organisatoriske tiltak for å sikre et sikkerhetsnivå som passer til de risikoer som er forbundet med behandlingen
- b. plikten til å anmelde brudd på personopplysningssikkerheten til tilsynsmyndigheten (Datatilsynet) uten unødig forsinkelse og om mulig senest 72 timer etter at den behandlingsansvarlige er blitt kjent med bruddet, medmindre at det er usannsynlig at bruddet på personopplysningssikkerheten innebærer en risiko for fysiske personers rettigheter eller frihetsrettigheter
- c. plikten til, uten unødig forsinkelse, å underrette den/de registrerte om brudd på personopplysningssikkerheten, når et slikt brudd sannsynligvis vil innebærer en høy risiko for fysiske personers rettigheter og frihetsrettigheter
- d. plikten til å gjennomføre en konsekvensanalyse vedrørende databeskyttelse, hvis en type behandling sannsynligvis vil innebærer en høy risiko for fysiske personers rettigheter og frihetsrettigheter
- e. plikten til å konsultere tilsynsmyndigheten (Datatilsynet) innen behandling, såfremt en konsekvensanalyse vedrørende personopplysningssikkerheten viser at behandlingen vil føre til høy risiko i mangel av tiltak truffet av den behandlingsansvarlige for å begrense risikoen

## 10. Varsel om brudd på personopplysningssikkerheten

10.1 Ved brudd på personopplysningssikkerheten hos databehandleren eller eventuell underdatabehandler, skal databehandleren uten ugrunnet opphold varsle den behandlingsansvarlige. Databehandlerens varsel til den behandlingsansvarlige skal om mulig skje senest 24 timer etter at denne er blitt kjent med bruddet, slik at den behandlingsansvarlige har mulighet for å etterleve sin eventuelle forpliktelse til å anmelde bruddet til tilsynsmyndigheten innenfor 72 timer. I overensstemmelse med denne avtales pkt. 9.2. litra b, skal databehandleren, hensyntatt behandlingens karakter og de opplysninger som er tilgjengelige for denne – bistå den behandlingsansvarlige med å anmelde bruddet til tilsynsmyndigheten.

Det kan bety at databehandleren bl.a. skal hjelpe med å fremskaffe nedenstående opplysninger, som etter personvernforordningens artikkel 33, nr. 3, skal fremgå av den behandlingsansvarliges anmeldelse til tilsynsmyndigheten:

- a. Karakteren av bruddet på personopplysningssikkerheten, herunder, hvis det er mulig, kategoriene og det omtrentlige antall berørte registrerte, samt kategoriene og det omtrentlige antall registreringer av personopplysninger
- b. Sannsynlige konsekvenser av bruddet på personopplysningssikkerheten
- c. Tiltak som er truffet eller foreslås truffet for å håndtere bruddet på personopplysningssikkerheten, herunder hvis det er relevant, tiltak for å begrense dets mulige skadevirkninger

## 11. Sletting og tilbakelevering av opplysninger

11.1. Ved opphør av tjenestene vedrørende behandling plikter databehandleren, etter den behandlingsansvarliges valg, å slette eller tilbakelevere alle personopplysninger til den behandlingsansvarlige, samt å slette eksisterende kopier, medmindre EU/EØS-retten eller nasjonal rett foreskriver oppbevaring av personopplysningene.

## 12. Tilsyn og revisjon

- 12.1. Databehandleren stiller alle opplysninger som er nødvendige for å påvise databehandlerens overholdelse av personvernforordningens artikkel 28, til rådighet for den behandlingsansvarlige og gir mulighet for og bidrar til revisjoner, herunder inspeksjoner, som foretas av den behandlingsansvarlige eller en annen revisor, som er bemyndiget av den behandlingsansvarlige.
- 12.2. Den behandlingsansvarliges tilsyn med eventuelle underdatabehandlere skjer som utgangspunkt gjennom databehandleren.
- 12.3. Databehandleren plikter å gi de myndigheter, som etter den til enhver tid gjeldende lovgivning har adgang til den behandlingsansvarliges og databehandlerens fasiliteter, eller representanter som opptrer på myndighetens vegne, adgang til databehandlerens fysiske fasiliteter mot gyldig legitimasjon.