GDPR – generel introduktion

Indhold

GDPR-brugervejledning – generel introduktion

Denne vejledning giver indledende information om, hvordan du overholder GDPR, når du arbejder med Wolters Kluwers softwareprodukter. For instruktioner helt ned på produkt niveau, henvises til vor Wolters Kluwer GDPR produkt manual. For generel information om GDPR og hvordan du overholder forordningen, anbefaler vi Datatilsynets vejledninger på www.datatilsynet.dk.

Denne vejledning forudsætter et arbejdskendskab til GDPR, og hvordan den påvirker de compliance processer, der understøttes af Wolter Kluwers produkter. Wolters Kluwer er i visse tilfælde (under)databehandler på vegne af sine kunder (dig). I disse tilfælde går Wolters Kluwer ud fra, at du, som vores kunde, har en lovlig grund til databehandlingen, og at du har kommunikeret, at Wolters Kluwer i visse tilfælde er (under)databehandler. Wolters Kluwer fungerer f.eks. som (under)databehandler i følgende tilfælde:

- Når Wolters Kluwer hoster produkter og data på dine vegne, via vores Citrix partner IT Forum.
- Når du, som dataansvarlig, sender data til Wolters Kluwer for support eller med produktforbedring som formål.

Det er den dataansvarliges ansvar at overholde GDPR. Wolters Kluwer vil hjælpe dig med at overholde GDPR ved hjælp af skriftlige instruktioner for vores forskellige løsninger, så du kan opfylde dine GDPR-forpligtelser.

Dataopbevaring

GDPR kræver, at du sletter personlige data, så snart du ikke længere har en god grund (lovlig grund) til at opbevare dem. Det betyder, at personlige data skal slettes, når f.eks. kontrakten med dine kunder ophører, eller når den registrerede ikke længere har en rolle i compliance processerne understøttet af Wolters Kluwers produkter. Der kan dog være tvingende grunde til at opbevare personlige data i en længere periode end GDPR tilsiger, nemlig overholdelse af den nationale lovgivning. I Danmark har vi således Revisorlovens § 23, der tilsiger at al dokumentation, fx i form af arbejdspapirer, der danner grundlag for erklæringer, skal opbevares i 5 år, samt bogføringsloven § 10, der fastlægger at bogførings- og regnskabsmateriale skal opbevares i 5 år.

I henhold til GDPR er det påkrævet, at I har en politik for opbevaring af personlige data på plads. Denne politik skal både overholde GDPR og andre love og bestemmelser. I skal også have processer på plads for at håndhæve denne politik, dvs. en proces for håndtering af personlige data når I bliver opmærksomme på, at I ikke længere har brug for dem. Wolters Kluwer vil, for hvert enkelt produkt, give konkrete vejledninger til, hvordan I håndterer GDPR reglerne i forhold til personlige data i Wolters Kluwers softwareprodukter.

Registreredes rettigheder

I henhold til GDPR har alle indbyggere i det Europæiske Økonomiske Samarbejde eksplicitte rettigheder i forhold til organisationer, der opbevarer deres personlige data. Denne sektion giver generel information om hver enkelt rettighed i forhold til Wolters Kluwers produkter. Wolters Kluwer vil også give konkrete vejledninger for hvert enkelt produkt vedrørende den registreredes rettigheder.

Transparens

Ved behandling af personlige data skal den dataansvarlige være transparent over for de registrerede om, hvilke personlige data der behandles og hvorfor (lovlig grund). Registrerede har også ret til at anmode om en oversigt over alle de personlige data, som du, som databehandler, behandler.

Indsigelse

Registrerede kan gøre indsigelse mod, at du, som dataansvarlig, behandler deres personlige data. Ved direkte markedsføring eller samtykkebaseret behandling skal disse anmodninger efterkommes. I andre tilfælde skal du, som dataansvarlig, være i stand til at give den registrerede en klar, lovlig grund for den fortsatte behandling eller efterkomme anmodningen. En efterkommelse af anmodningen vil føre til enten sletning eller begrænsning (se følgende sektioner for yderligere oplysninger).

Sletning – "retten til at blive glemt"

Registrerede kan anmode om, at du, som dataansvarlig, sletter alle deres personlige data, herunder personlige data, der behandles af databehandlere på den dataansvarliges vegne. En sådan anmodning skal efterkommes, hvis du, som dataansvarlig, ikke længere har en klar, lovlig grund til at behandle dataene.
Det er ikke nødvendigt også at slette personlige data fra backups. Men, når du gendanner en backup, skal du sørge for, at personlige data, der blev slettet efter backuppen blev lavet, slettes igen efter gendannelsen. Den nemmeste måde at gøre det på er ved at gemme en fortegnelse over alle sletninger af personlige data med tids stempel og identificering og at bruge denne fortegnelse til at slette igen (eller anonymisere igen) efter en gendannelse.

Begrænsning

Registrerede kan bede om begrænsning i brugen af deres personlige data i stedet for at få dem slettet. I dette tilfælde må du, som dataansvarlig, ikke længere bruge (behandle) disse personlige data, men du er ikke forpligtet til at slette dem. Både du, som dataansvarlig, og den registrerede kan have tvingende grunde til ikke at slette de personlige data, også selvom du ikke længere må behandle dem. I dette tilfælde skal du bruge en måde, hvorpå du kan "deaktivere" personlige data uden at slette dem. Her skal du også have en fortegnelse over de deaktiverede data for at kunne deaktivere de personlige data igen efter gendannelse af en backup.

Berigtigelse

Dataansvarlige skal gøre det nemt for de registrerede at rette/fuldstændiggøre deres personlige oplysninger. Det har dog altid været meget vigtigt at have korrekte og komplette personlige data, når man arbejder med compliance processer understøttet af Wolters Kluwers produkter, så dette bør ikke føre til nye krav.

Dataportabilitet

Registrerede kan under visse betingelser anmode om at få udleveret deres personlige data i et maskinlæsbart format. Wolters Kluwers holdning er, at det er usandsynligt, at den registreredes ret til dataportabilitet bliver relevant, når det gælder compliance processerne understøttet af Wolters Kluwers softwareprodukter.

Informationssikkerhed

GDPR kræver også, at du, som dataansvarlig, gennemgår din informationssikkerhed og – hvis nødvendigt – som minimum forbedrer den til "markedsstandard". Det er især vigtigt, når du behandler følsomme personoplysninger, hvilket ofte er tilfældet, når du arbejder med compliance processer såsom selvangivelser, årsafslutning og revision.
Datafiler og databaser oprettet og brugt af Wolters Kluwers softwareprodukter er ikke (stærkt) krypterede. Det betyder, at du, som dataansvarlig, skal indføre yderligere informationssikkerhedsforanstaltninger for at sikre disse data.
Brug ikke bærbare lagringsenheder (usb-drev osv.) til opbevaring af personlige data. Hvis du alligevel bruger usb-drev eller andre bærbare lagringsenheder, så skal du sikre, at enheden er krypteret, så dataene på den ikke kan læses af andre i tilfælde af tab eller tyveri.
Sørg for, at (personlige) data, der opbevares på slutbrugerenheder såsom computere, bærbare computere, tablets og mobiltelefoner, er krypterede. Alle moderne operativsystemer understøtter kryptering af enheder; dette skal aktiveres på alle enheder, der kan indeholde personlige data i enhver form (inklusive e-mails og dokumenter).
Sørg for, at hele dit IT-miljø er beskyttet mod virus og anden skadelig software. Det er ikke kun computere og bærbare computere, der skal beskyttes, også mobile enheder og servere.
Sørg for, at dit netværk og dine servere er sikre. Dette inkluderer fysisk sikkerhed (faciliteter) og kommunikationssikkerhed såsom firewalls, indbrudsdetektering/-beskyttelse og trådløs netværkssikkerhed. Du kan gøre dine servere ekstra sikre ved også at kryptere de (personlige) data, der opbevares på dem. Backup-filer, der indeholder personlige data, skal også krypteres.
Brug ikke gratis cloud-tjenester til at opbevare eller dele personlige data. Når du bruger cloud-tjenester til at opbevare personlige data, skal du sikre dig, at dataene ikke forlader EØS-området, og at både cloud-udbyderen og den kontrakt, du har med denne udbyder, overholder GDPR.

Samarbejde

Særlig opmærksomhed er påkrævet, når du samarbejder med kunder, kollegaer, leverandører og tredjeparter i compliance processen, understøttet af Wolters Kluwers softwareprodukter. Det er således ikke sikkert at sende data ukrypteret via e-mail eller SMS-apps. Det samme gælder for deling af filer via gratis cloud-tjenester.
En anbefalet måde at samarbejde på er, at bruge en sikker fildelingsløsning. Der er flere leverandører, som tilbyder sikre fildelingsløsninger, der overholder GDPR.
Hvis du vælger ikke at bruge en sådan sikker fildelingsløsning, er anbefalingen, at du i det mindste krypterer filerne, før du deler dem (f.eks. ved at bruge password-beskyttet filkomprimering). Hvis du beslutter at anvende e-mails, er anbefalingen således også at anvende kryptering. Sørg i dette tilfælde for at (1) sende dekrypteringsnøglen/passwordet i en separat besked, at (2) bruge forskellige dekrypteringsnøgler/passwords til forskellige samarbejdspartnere og at (3) ændre dekrypteringsnøgler/passwords regelmæssigt.