GDPR – generell introduktion

Innehåll

Användarhandbok för GDPR – generell introduktion

I den här handboken kan du läsa mer om hur du gör för att följa GDPR när du arbetar med Wolters Kluwers programvaruprodukter. Mer allmän information om dataskyddsförordningen GDPR och hur du följer den finns på Bolagsverkets GDPR-guide på verksamt.se. Om du vill veta mer om vad Wolters Kluwer gör i förhållande till GDPR kan du besöka vår webbplats.
Handboken förutsätter att du har grundläggande kännedom om GDPR och hur det påverkar de processer för regelefterlevnad som Wolters Kluwers produkter ger stöd för. Wolters Kluwer är i vissa fall personuppgifts(under)biträde åt sina kunder (t.ex. dig). I dessa fall förutsätter Wolters Kluwer att du som kund har en rättslig grund för behandlingen och att du har informerat om att Wolters Kluwer är personuppgifts(under)biträde i vissa fall. Wolters Kluwer har rollen som personuppgifts(under)biträde i bland annat följande fall:

- När Wolters Kluwer hyser produkter och data för din räkning, till exempel via Citrix.
- När du som personuppgiftsansvarig skickar data till Wolters Kluwer för supportärenden eller i produktförbättringssyfte.

Det är personuppgiftsansvarigs ansvar att följa GDPR. Wolters Kluwer bistår dig med skriftliga instruktioner till våra olika lösningar för att hjälpa dig att uppfylla dina åtaganden enligt GDPR.

Lagring av uppgifter

GDPR kräver att du raderar personuppgifter så snart du inte längre har goda skäl (rättslig grund) att lagra dem. Det innebär att alla uppgifter måste raderas till exempel när kontraktet med din kund upphör eller när den registrerade upphör att fylla en funktion i de processer för regelefterlevnad som Wolters Kluwers produkter ger stöd för. Observera att det kan finnas starka skäl för att behålla personuppgifter längre än så, till exempel för att följa Lag om Penningtvätt, Bokföringslagen och Revisionslagen.
Enligt GDPR är du skyldig att ha en lagringspolicy för personuppgifter. Policyn måste följa både GDPR och andra lagar och förordningar. Du måste också ha etablerade rutiner för att tillämpa din lagringspolicy, det vill säga radera eller anonymisera personuppgifter när du inser att du inte längre behöver dem. Wolters Kluwer kommer att tillhandahålla specifika guider för alla sina produkter om hur du raderar eller – när detta är aktuellt – anonymiserar personuppgifter.

Registrerades rättigheter

Enligt GDPR har alla invånare i Europeiska ekonomiska samarbetsområdet (EES) uttryckliga rättigheter i förhållande till organisationer som lagrar personuppgifter om dem. I det här avsnittet följer allmän information om dessa rättigheter i förhållande till Wolters Kluwers produkter. Wolters Kluwer kommer också att tillhandahålla specifika guider för alla sina produkter om de registrerades rättigheter.

Transparens

När man behandlar personuppgifter måste personuppgiftsansvarig vara transparent gentemot de registrerade kring vilka personuppgifter som behandlas och varför (rättslig grund). De registrerade har också rätt att begära en sammanställning av alla personuppgifter som du som personuppgiftsansvarig behandlar.

Invändning

De registrerade har rätt att invända mot hur du som personuppgiftsansvarig behandlar deras personuppgifter. När det gäller direkt marknadsföring eller behandling som grundar sig på samtycke måste du tillmötesgå denna begäran. I övriga fall måste du som personuppgiftsansvarig antingen kunna ge den registrerade en tydlig rättslig grund för fortsatt behandling eller tillmötesgå deras begäran. Att tillmötesgå en invändning innebär att antingen radera eller begränsa behandlingen av personuppgifterna (mer information finns i följande avsnitt).

Radering – ”rätten att bli bortglömd”

De registrerade kan begära att du som personuppgiftsansvarig ska radera alla deras personuppgifter, inklusive uppgifter som personuppgifts(under)biträden behandlar för personuppgiftsansvarigs räkning. En sådan begäran måste alltid beviljas om du som personuppgiftsansvarig inte längre har en tydlig rättslig grund för behandlingen. Radering av personuppgifter kan också uppnås genom anonymisering.
Det är inte nödvändigt att även radera personuppgifterna från säkerhetskopior. Om du däremot gör en återställning från en säkerhetskopia måste du se till att personuppgifterna som har raderats sedan säkerhetskopian togs blir raderade på nytt efter återställningen. Enklaste sättet att göra detta är att ha en loggfil med alla raderingar av personuppgifter med tidsstämpel och identifikatorer och att använda den loggfilen för ny radering (eller anonymisering) efter en återställning.

Begränsning

Istället för radering kan de registrerade också begära begränsning. Då får du som personuppgiftsansvarig inte längre använda (behandla) personuppgifterna, men du är inte skyldig att radera dem. Både den registrerade och du som personuppgiftsansvarig kan ha starka skäl att inte radera personuppgifterna, även om du inte längre får lov att behandla dem. I ett sådant fall behöver du ha ett sätt att ”inaktivera” personuppgifterna utan att radera dem. Även här behöver du ha en loggfil med inaktiverade personuppgifter så att du kan göra om inaktiveringen efter en återställning från säkerhetskopia.

Rättelse

Personuppgiftsansvariga måste erbjuda ett enkelt sätt för de registrerade att rätta eller komplettera sina personuppgifter. Att ha korrekta och fullständiga personuppgifter har alltid varit av största vikt för de processer för regelefterlevnad som Wolters Kluwers produkter ger stöd för, och därför bör detta inte medföra några nya krav.

Portabilitet

De registrerade kan under vissa omständigheter begära ut en maskinellt läsbar kopia av sina personuppgifter. Wolters Kluwers uppfattning är att de registrerades rätt till portabilitet knappast kommer att bli relevant inom ramen för de processer för regelefterlevnad som Wolters Kluwers programvaror ger stöd för.

Informationssäkerhet

GDPR kräver också av dig som personuppgiftsansvarig att du ser över din informationssäkerhet och vid behov förbättrar den till ”marknadsstandard” som minimum. Detta är särskilt viktigt när man hanterar känsliga personuppgifter, vilket ofta är fallet när man arbetar med processer för regelefterlevnad som skatteredovisning, bokslut och revision.

De datafiler och databaser som skapas och används av Wolters Kluwers programvaror är inte (starkt) krypterade. Det innebär att du som personuppgiftsansvarig måste vidta ytterligare informationssäkerhetsåtgärder för att säkra dessa uppgifter.
Använd aldrig portabla lagringsmedier (USB-minnen och liknande) för att lagra personuppgifter. Om du ändå använder USB-minnen eller andra portabla lagringsmedier bör du se till att dessa är krypterade så att uppgifterna inte kan läsas av obehöriga vid eventuell stöld eller förlust.
Se till att (person)uppgifter som lagras på slutanvändarnas enheter, till exempel datorer, surfplattor och mobiler, är krypterade. Alla moderna operativsystem stöder kryptering. Detta måste aktiveras på alla enheter som kan innehålla personuppgifter i någon form (inklusive e-post och dokument).
Se till att hela IT-miljön är skyddad mot virus och annan skadlig programvara. Det är inte bara stationära och bärbara datorer som måste skyddas, utan även mobila enheter och servrar.
Se till att ditt nätverk och dina servrar är säkra. Detta inkluderar även fysisk säkerhet (anläggningssäkerhet) och kommunikationssäkerhet som brandväggar, intrångsdetektering och intrångsskydd samt säkerhet för trådlösa nätverk. Du kan även öka serversäkerheten ytterligare genom att tillämpa kryptering på (person)uppgifter som lagras på servrar. Säkerhetskopierade filer som innehåller personuppgifter måste också krypteras.
Lagra eller dela aldrig personuppgifter på gratis molntjänster som Dropbox, OneDrive, iCloud eller Google Drive. När du använder molnlagringstjänster för att lagra personuppgifter måste du se till att uppgifterna aldrig lämnar EES och att både leverantören av molntjänsten och avtalet som du har med den leverantören helt och håller följer GDPR.

Samarbete

Var särskilt uppmärksam när du samarbetar med kunder, kollegor, leverantörer och tredje part inom de processer för regelefterlevnad som Wolters Kluwers programvaror ger stöd för. Att skicka datafiler via e-post eller meddelandeappar är inte säkert, inte heller att dela filer via kostnadsfria bastjänster för molnlagring.
Det bästa är att samarbeta via en säker fildelningslösning. Det finns flera olika leverantörer som erbjuder säkra fildelningslösningar som följer GDPR. Om du inte kan använda en säker fildelningslösning måste du åtminstone kryptera filerna innan du skickar dem, till exempel med hjälp av lösenordsskyddad filkomprimering. Var noga med att (1) skicka krypteringsnyckeln/lösenordet i ett separat meddelande, (2) använda olika krypteringsnycklar/lösenord för olika samarbetspartner och (3) byta krypteringsnyckel/lösenord regelbundet.