GDPR Veiledning

for

Visma Contracting

Oslo Mai 2018

Versjon 1.0

1.0 Hva betyr GDPR

EUs *forordning* for personvern, (General Data Protection Regulation), blir norsk lov i løpet av 2018, og erstatter da dagens regelverk. Vi får med andre ord nye regler for personvern i Norge. De gir virksomheter nye plikter, og personene man behandler personopplysninger om, de registrerte, får nye rettigheter. Dagens regelverk stiller krav til at virksomheten skal ha rutiner for å etterleve personopplysningsloven. Når loven endres, må virksomheten også endre disse rutinene. De nye rutinene skal sørge for at dere følger de nye pliktene dere vil få etter ny lov. Det er virksomhetens ledelse som har ansvaret for å utforme de nye rutinene, men alle i organisasjonen må kjenne til og følge de nye reglene.

1.1 Hvem vil innføringen av GDPR påvirke?

Innføringen av GDPR i EU og EØS vil ikke bare gjelde for organisasjoner som befinner seg innenfor disse landene, men det vil også gjelde for organisasjoner som ligger utenfor området hvis de tilbyr varer eller tjenester til EU/EØS. Det gjelder for alle selskaper sin behandling av personlige data for å ivareta enkeltpersoner sitt personvern.

1.2 Hva gjør Visma i forhold til GDPR?

Visma har naturligvis satt seg som mål å sikre at alle våre programvaretjenester, er i samsvar med det nye GDPR regelverket. Visma har derfor utviklet et omfattende rammeverk spesielt med tanke på GDPR som består av følgende hovedkomponenter:

- Opplæring for våre ansatte
- Personvern og databeskyttelse innebygd i utvikling og produksjon
- Utnevnt en “Data Protection Manager”
- Oppdatert Bruks & Vedlikeholdsavtalene for programvaretjenester

1.3 Hva utgjør personopplysninger?

All informasjon knyttet til en fysisk person eller 'Data Subject', som kan brukes til å direkte eller indirekte identifisere personen utgjør personopplysninger. Det kan være alt fra et navn, et bilde, en e-postadresse, bankinformasjon, innlegg på sosiale nettverk eller nettsteder, medisinsk informasjon, eller en datamaskin sin IP-adresse.

Visma som leverandør av skyløsninger og lokalt installert programvare fokuserer på hvordan vi kan tilrettelegge i vår programvare for å sikre at kunder vil være i stand til å overholde de nye forskriftene. Dette dokumentet skal gi veiledning for Visma Contracting kunder for å sette opp systemet og gi veiledning og råd om hvordan brukerne av systemet kan tilfredsstille GDPR regelverket.

Det er også viktig å forstå at programvaren i seg selv ikke trenger å overholde GDPR; det er alltid virksomheten som bruker systemet som trenger å sikre at alle prosesser, inkludert måten de bruker programvare på er i samsvar med det nye regelverket.

Dette dokumentet alene kan ikke brukes som en akseptkriterie sett i forhold til GDPR. Det er også meget vanlig at andre systemer, (ikke Visma systemer), er i bruk og lagrer personlige eller sensitive data. Hver bedrift har derfor behov for å kontrollere sin egen praksis på dette området og kontrollere at de har en prosess på plass som er i tråd med GDPR.

Dokumentet vil kun fokusere på Visma Contracting og hva som må vurderes når du benytter denne programvaren.

Visma Contracting er ofte også integrert med Visma sine skytjenester, som Visma .net AutoInvoice eller Visma.net Approval. I løpet av de kommende årene vil vi se enda mer funksjonalitet flyttet fra lokalt installert programvare til skytjenester. Mer informasjon om sikkerhet og personvern kan bli funnet her:

- https://www.visma.com/privacy/
- https://www.visma.com/trust-centre/

Veiledningen som beskrives i dette dokumentet vedrører et såkalt “On Premise” miljø (lokalt installert programvare på Windows-operativsystem). Det betyr at hvert selskap som bruker Visma Contracting må ta eierskap og ansvar for sikkerheten og miljøet der programvaren er installert og driftes, og hvert selskap har det overordnede ansvar for å dekke kravene til GDPR. Visma sin rolle er å tilby programvare som gjør det mulig å overholde regelverket og gi retningslinjer og verktøy for å gjøre det lettere for et selskap å følge GDPR regelverket.

2.0 GDPR og Visma Contracting

Målet med GDPR er å beskytte alle EU-borgere med hensyn til personvern og mot datainnbrudd / misbruk i en stadig mer datadrevet verden som er svært forskjellig fra den tiden der 1995 direktivet ble etablert. Selv om hovedprinsippene for personvern fortsatt støtter seg til det forrige direktivet, har det skjedd mange endringer innenfor den teknologiske utviklingen. De viktigste punktene i GDPR, samt kunnskap om hvilke betydning det vil få for å ivareta personvernet finner du nedenfor.

2.2 Personlige rettigheter og funksjonalitet

Følgende liste oppsummerer de mest relevante rettighetene privatpersoner har, som kan bli aktuelle i forbindelse med registrering og lagring av personopplysninger ved bruk av Visma Contracting:

2.2.1 Retten til informasjon og innsyn.

Ved en eventuell forespørsel fra en privatperson må det, om nødvendig, kunne gis følgende opplysninger:

- Kontaktinformasjon til den data ansvarlige i virksomheten
- Kontaktdetaljer til et eventuelt personvernombud (for store virksomheter)
- Hva som er formålet med behandlingen av personopplysningene
- Hva slags personopplysninger som behandles
- Formålet for behandlingen av personopplysninger
- Hvem personopplysningene eventuelt leveres ut til
- Hvor lenge de personlige opplysningene skal oppbevares
- At den registrerte har rett til innsyn, retting, sletting og dataportabilitet om grunnlag for dette foreligger.
- At den registrerte har rett til å klage til Datatilsynet på behandling i strid med reglene

En del av de utvidede registrertes rettigheter skissert av GDPR er den retten til å få opplysninger om data som er registrert i systemet fra behandlingsansvarlige. Det skal kunne skrives ut en bekreftelse på hvorvidt personopplysninger er registrert, om de blir behandlet, hvor de blir behandlet og til hvilket formål. Videre skal databehandleren tilgjengeliggjøre en kopi av personlige data, uten omkostninger, i et elektronisk format. Denne endringen er en dramatisk endring i data åpenhet og styrking av personvernlovgivningen.

I mange tilfeller har Visma Contracting privatpersoner registrert som kunder. I dette tilfellet kan du skrive ut en kundeliste som du finner i menyen Regnskap - Kunder - Lister - Kundelister for å ta ut en rapport på de private opplysningene som foreligger. Her kan du gjøre et utvalg på den aktuelle kunden. Denne rapporten kan skrives ut på papir eventuelt i pdf format og sendes på mail til den som forespør.

Det anbefales i tillegg å utarbeide et generelt skriv, (følgeskriv), som gir generelle opplysninger i henhold til punktene ovenfor om kontaktinformasjon, hvilket formål, rett til innsyn og klagerett til datatilsynet etc.

2.2.2 Retten til å bli glemt

Retten til å bli glemt gir den registrerte mulighet til å forespørre data-ansvarlig i virksomheten til å slette hans/hennes personlige opplysninger, stoppe ytterligere spredning av data, og potensielt sørge for at tredjepartsprogrammer stanser behandlingen av data. Betingelsene for sletting, som beskrevet i artikkelen 17, innbefatter de data som ikke lenger er relevant for opprinnelige formål for behandling. Det bør også bemerkes at "retten til å bli glemt" krever en fagmessig vurdering, av "retten til å bli glemt", opp i mot myndighetenes interesse, i form av bokettersyn av regnskap/revisjon og tilgjengeligheten av aktuelle data.

I Visma Contracting kan du slette personlig informasjon ved bruk av standard rutiner for å slette data om plikten til å slette foreligger, og det ikke lenger er formålstjenlig å beholde dataene. Fra myndighetenes side foreligger det også krav ut over regnskapsplikten til å dokumentere hvilke kunder som har fått levert f. eks. vvs/elektro-varer hvor det i ettertid kan oppdages feil på utstyr som må utbedres. Det vil i slike situasjoner være formålstjenlig for virksomheten å lagre personopplysningene ut over 5 år som er kravet i forhold til bokføringsloven og utover 10 år som er minimum bransjestandard.

2.2.3 Dataportabilitet

GDPR innfører dataportabilitet som en personvernrettighet som innebærer at personopplysninger om dem, som de tidligere har tilveiebragt skal kunne leveres i et "standard elektronisk maskinlesbart format slik at data kan overføres til et annet system.

I Visma Contracting kan du benytte deg av standard funksjonalitet for å skrive til Excel/csv-format slik at retten til dataportabilitet kan ivaretas.

2.2.4 “Privacy by design”

“Privacy by design”, eller personvern-fokus i utviklingsarbeidet, er et begrep som har eksistert i mange år, men det er først nå det er blitt en del av et juridisk krav med innføringen av GDPR. Grunntanken her er at under utvikling og produksjon av programvaren skal fokuset være på å beskytte personlige opplysninger som finnes i systemet mot eventuelle “hackerangrep” fra utsiden og skal være som standard adgangsregulert.

2.2.4.1 *proaktiv og forebyggende*

Visma Contracting sin utviklingsavdeling er en del av en “ISO 9001: 2015” sertifisert organisasjon. Dette sikrer at vi har et godkjent system for kvalitetsstyring på plass med et definert sett med retningslinjer, prosesser og prosedyrer som kreves for planlegging og gjennomføring av utviklingsarbeidet. Dette betyr at før hver utgivelse av en Visma Contracting sin hoved versjonen har vi gjort tilstrekkelig mengde testing, pilotering og stabilisering for å proaktivt hindre at sikkerhetsproblemer oppstår når kundene implementerer den nye versjonen.

Vi anbefaler Visma Contracting kunder å lære opp ansatte (databehandlere) i bruken av systemet med tanke på sikkerhet, og implementere et kvalitetsstyringssystem, ved siden av, som inkluderer roller og prosedyrer for å proaktivt beskytte privat eller sensitiv personlig informasjon i systemet.

2.2.4.2 *Personvern som standardinnstilling*

Gjennom standard tilgangsstyring i Visma Contracting sikres det at bare autoriserte identifiserbare navngitte brukere har tilgang til dataene. Adgangskontrollsystemet gjør det mulig for brukeren å ha ulike tilgangsnivåer og forskjellige områder av tilgang. (Se Visma Contracting brukerdokumentasjon for mer informasjon rundt dette)

Vi anbefaler systemadministratoren å sette opp en streng tilgangskontroll, med bruk av sterkt passord (som også kan inneholde spesialtegn), men maks 8 tegn til sammen,

2.2.4.3 “Privacy” innebygd i utformingen

Visma Contracting som standard lagrer ikke sensitive data, men systemet tillater brukere å legge inn data av sensitiv karakter hvis de velger å gjøre det. Registrering av data av en slik art er kundens eget ansvar og kan ikke kontrolleres av leverandøren av systemet.

2.2.4.4 Full funksjonalitet

Adgangskontrollen og systemfilen til sammen sørger for at brukerne bare gis tilgang til data eller moduler som er relevant og nødvendig for databehandlingen.

2.2.4.5 *Ende-til-ende-sikkerhet*

Ved bruk av Visma Contracting må alle kunder, før systemet tas i bruk, signere en ABV avtale (Avtale om Bruksrett og Vedlikehold) som bl.a. sier: "Kunden er forpliktet til å benytte den nyeste versjonen av den leverte Programvaren." Kunden må også sørge for oppdatert infrastruktur med de nyeste Operativsystemer og sikkerhetsoppdateringer.

"Ende-til-ende-sikkerhet" konseptet består ikke bare av sikker og korrekt registrering av personopplysninger, men også beskyttelse av personlige data i kundens miljø, under den daglige behandlingen. Til slutt handler dette punktet i personvern om sikker fjerning eller sletting av data når dataene ikke lenger er relevant eller formålstjenlig å beholde.

2.2.4.6 Respekt for personvern

Visma Contracting som et "On Premise", (lokalt installert programvare), gir ikke direkte tilgang til privatpersoner for å kontrollere, redigere eller slette sine egne personlige data.

Ved en eventuell henvendelse til data-ansvarlig i virksomheten kan en rapport om de personlige data som foreligger skrives ut på papir, eventuelt til pdf og sendes på e-post til den som forespør. Videre kan data redigeres av en bruker med tilgang til systemet om personlig informasjon skulle være feil.

2.3 Behandling av data i Visma Contracting

Visma Contracting blir levert med et standard sett av datafiler med innhold som kan brukes til å lagre og behandle data. Hvis standard-feltene ikke blir brukt til standard formål, (hovedformålet med feltet), så vil funksjonaliteten i Contracting i seg selv ikke være tilstrekkelig nok til å overholde GDPR krav, da det ikke finnes funksjonalitet for å validere hva brukeren registrerer av informasjon i systemet. Dette gjelder ikke bare de vanlige feltene men også fritekstfelt eller notater/meldinger samt annen vedlagt dokumentasjon.

Programvare levert av Visma i GDPR sammenheng er avhengig av standard bruk av systemet og overlater ansvaret til databehandleren og sikkerhetsrutinene rund systemet for å ivareta regelverket for personvern. Ved normal bruk av Visma Contracting, er det ingen sensitive personopplysninger som er lagret i systemet.

Det anbefales at virksomheten gjennomgår rutinene for registrering av data inn i systemet for å identifisere eventuelle sensitive data. Virksomheten må sørge for at

informasjonen kun er tilgjengelig for autorisert personell, eller databehandlere som trenger tilgang til disse dataene for å fullføre sine daglige oppgaver.

Om en virksomhet behandler sensitive personopplysninger i stor skala, så er det behov for å oppnevne en Data Protection Officer (DPO). DPO må involveres når det fattes vedtak om hvilke sensitive personopplysninger skal lagres i Visma Contracting og hvordan tilgangen skal adgangsreguleres.

I henhold til GDPR-regelverket skal lønnsslipper fra Visma Contracting kun sendes til lønnstakernes e-postadresser i virksomheten. Det anbefales ikke å sende ukrypterte lønnsslipper til private e-postadresser utenfor bedriftens domene eller via Microsoft Office 365.

2.4 Lagring av data med personopplysninger

Visma Contracting kan lagre personopplysninger på følgende steder:

- Datafiler som inneholder personopplysninger lagres kun på virksomhetens server og på de backup-media den til enhver tid måtte benytte.
- Lokalt lagrede filer/vedlegg kan inneholde personlig informasjon
    - I Contracting, er det mulig å gjøre flere innstillinger av filbaner som vil bestemme hvor filene skal lagres på virksomhetens server (f.eks. lønns dokumenter).
    - Dataansvarlig må påse at sikkerheten rundt delte mapper er slik at de kun er tilgjengelig for autorisert personell.
    - Loggfiler lagres i Data-mappe på virksomhetens server, men inneholder ikke personopplysninger.

Lagring av sikkerhetskopier:

- Det anbefales å sikkerhetskopiere data som produseres av Visma Contracting på jevnlig basis. Sikkerhetskopier og filer lagret lokalt er også gjenstand for GDPR bestemmelser om beskyttelse av data.

Bruk av sikkerhetskopier:

- Ved utlevering av sikkerhetskopier av data, bør virksomheten utarbeide spesielle retningslinjer for å sikre at personopplysninger ikke kommer på avveie.

2.5 Datautveksling på tvers av Visma applikasjoner/tjenester

Visma Contracting kan være integrert med annen lokalt installert programvare eller skytjenester.

Det finnes hovedsaklig to typer datautveksling:

- Andre Visma programmer lokalt installert som Visma Dokumentsenter og ERP POS.
- Visma-eide skytjenester knyttet til lokalt installerte produkter som Visma.net AutoInvoice, Visma.net Approval og Autocollect.

Visma bestreber seg på å gi best mulig datasikkerhet til alle hybrid-kombinasjoner mellom systemene. For ytterligere spørsmål eller mer detaljert informasjon, vennligst ta kontakt med oss på trust@visma.com.

2.6 Datautveksling / deling av data med 3dje parts programvare

Visma Contracting har en rekke 3dje parts applikasjoner som vi normalt utveksler data med. Dette er også underlagt GDPR fordi informasjonen deles med tredjeparter. Hvert selskap må ha rutiner på plass for å dekke disse scenarioene. Det er opp til hvert enkelt selskap å definere sin egen prosess for å overholde GDPR når data deles med tredjeparter.

Ta eventuelt kontakt med leverandør av 3dje parts programvare for å få informasjon om hvordan personvern og datasikkerhet er ivaretatt.

2.7 Forespørsler om å fjerne personlige data

En privatperson kan be om å fjernet personlige data hvis systemet inneholder privat informasjon. Disse forespørslene må behandles i forhold til den til enhver tid gjeldende regnskapslov. Regnskapslovens bestemmelser om lagring/oppbevaring av data overstyrer GDPR-regelverket.