Crona Lön och GDPR

DataVara AB

Syftet med personregistret i Crona Lön

Supportdokument nr: LON0151
Programvara: Crona Lön, Modell: Alla

Bakgrund

När man använder programvaror som ingår i vår programserie Crona Lön sparas personuppgifter.

All behandling av personuppgifter måste uppfylla de grundläggande principer som anges i dataskyddsförordningen (GDPR). Principerna innebär bland annat att personuppgifter bara får samlas in för berättigade syften och att mängden uppgifter ska begränsas till vad som är nödvändigt för syftet.

Uppgifterna får inte senare behandlas på ett sätt som är oförenligt med dessa syften och inte heller sparas längre än nödvändigt.

Den som behandlar personuppgifter ska ansvara för och kunna visa att man följer bestämmelserna i dataskyddsförordningen (ansvarsskyldighet).

Rättslig grund

För att det ska vara tillåtet att alls behandla personuppgifter måste det alltid finnas ett stöd i dataskyddsförordningen, en så kallad *rättslig grund*. En sådan rättslig grund är samtycke från den registrerade. Andra rättsliga grunder är om personuppgiftsbehandlingen är nödvändig för att fullgöra ett avtal med den registrerade, fullgöra en rättslig förpliktelse, skydda den registrerades grundläggande intressen, fullgöra en uppgift av allmänt intresse, för myndighetsutövning, samt efter en intresseavvägning.

Syftet med personregistret

Den rättsliga grunden för att spara personuppgifter i Crona Lön bygger på just rättslig förpliktelse.

Som arbetsgivare krävs lagring av personuppgifter för att kunna betala ut lön, redovisa information till banken, Skatteverket, Försäkringskassan, fackföreningen och en mängd andra organisationer. Detta är lagbundet eller avtalat.

Även förtroendeuppdrag inom företagets verksamhetsområde som t.ex. skyddsombud, facklig företrädare eller annat är också information som kan komma att sparas om en person av samma skäl som ovan.

Information som kan underlätta en medarbetares karriärsutveckling och för företagets rekrytering kan också komma att sparas, dvs. vilka baskunskaper som finns, erfarenheter, befattning, branschvana och noteringar om genomgånga utbildningar, etc.

Rätt använd sparas i Crona Lön ingen information som inte behövs för att fullgöra företagets åtagande enligt ovan.

Crona Lön begränsar givetvis inte möjligheten att i fritextfält och liknande skriva vadhelst man önskar. Det är då upp till den personuppgiftsansvarige att reglera detta och hantera det rättsligt.

Samtycke krävs inte

Inga uppgifter i Crona Lön, förutom möjligtvis bild på en medarbetare, kräver samtycke enligt dataskyddsförordningen. All information i Crona Lön vilar på rättslig förpliktelse.

Samtyckesavtal

Det kan ändå vara lämpligt att teckna ett samtyckesavtal med var och en av företagets medarbetare. Det finns säkert andra system, program och områden med personregister där syftet med registret är av den arten att samtycke krävs. Lämpligt är att man har ett och samma avtal med en medarbetare som omfattar företagets alla sparade personuppgifter.

Uppgifter om en anställd och kanske bild kan också komma att användas i företagets utåtriktade verksamhet, dvs. på hemsidor, i företagspresentationer, etc. Den typen av personuppgifter kräver samtycke.

Eget samtyckesavtal

Personuppgifter får alltså behandlas om man har ett samtycke från den som personuppgifterna avser.

I dataskyddsförordningen ställs det särskilda krav på samtycket, bland annat att det ska vara frivilligt, att det ska lämnas genom ett uttalande eller en entydig bekräftande handling och att det ska ges efter att den registrerade har fått information om personuppgiftsbehandlingen.

Den som behandlar personuppgifter med stöd av ett samtycke måste kunna visa att ett giltigt samtycke har lämnats av den registrerade.

Blanketter i Dokumentpanelen

I Crona Lön och dess dokumentpanel finns ett antal blanketter tillgängliga, bl.a. ett *Samtyckesavtal*. Det är ett förslag på skrivning som kan ändras och komplettera efter eget önskemål.

Där finns också förslag på personuppgiftsbiträdesavtal och avtal för underbiträden. Möjlighet finns för tillägg i dessa blanketter.

Det är den personuppgiftsansvarig som ska bedöma i den mån dessa blanketter är tillfylles för det ändamål som de ska användas. Er branschorganisation kanske har andra varianter?

Dataskyddsförordningen och olika roller

Supportdokument nr: LON0155
Programvara: Crona Lön, Modell: Alla

Den som behandlar personuppgifter är antingen *personuppgiftsansvarig*, *personuppgiftsbiträde* eller *underbiträde*.

Personuppgiftsansvarig är den som bestämmer för vilka ändamål uppgifterna ska behandlas och hur behandlingen ska gå till. Personuppgiftsbiträde och underbiträdet är de som behandlar personuppgifter för den personuppgiftsansvariges räkning.

En personuppgiftsansvarig eller ett personuppgiftsbiträde kan vara en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ.

Personuppgiftsansvarig

Personuppgiftsansvarig är den organisation som bestämmer för vilket ändamål uppgifterna ska behandlas och hur den ska gå till. Det är alltså är inte chefen på en arbetsplats eller en anställd som är personuppgiftsansvarig. Även en fysisk person kan vara personuppgiftsansvarig som för en enskild firma.

Den som är personuppgiftsansvarig kan överlåta den behandlingen av personuppgifter men ansvaret kan aldrig överlåtas.

Den personuppgiftsansvarige måste se till att behandlingen sker i enlighet med dataskyddsförordningens samtliga bestämmelser. Dess personal får enbart behandla personuppgifter enligt de instruktioner som getts av den personuppgiftsansvarige.

Den personuppgiftsansvarige har ett generellt ansvar att, utifrån de integritetsrisker som finns med behandlingen, genomföra lämpliga tekniska och organisatoriska åtgärder för att säkerställa och kunna visa att behandlingen utförs i enlighet med dataskyddsförordningen.

Detta kan vara att man har antagit en policy med strategier för dataskydd och ser till att genomföra den. Uppförandekoder och certifieringar kan vara ett annat sätt att visa att man uppfyller dataskyddsförordningens bestämmelser.

Personuppgiftsbiträde

Personuppgiftsbiträde är den som behandlar personuppgifter för en personuppgiftsansvarigs räkning. Ett personuppgiftsbiträde finns alltid utanför den personuppgiftsansvariges organisation. Ett personuppgiftsbiträde kan vara en fysisk eller juridisk person. De biträden som den personuppgiftsansvarige anlitar ska kunna ge tillräckliga garantier för att behandlingen uppfyller kraven i dataskyddsförordningen och säkerställer att den registrerades rättigheter skyddas.

Ett personuppgiftsbiträde och dess personal får enbart behandla personuppgifter enligt instruktion från den personuppgiftsansvarige. Biträdet får inte anlita ett annat biträde utan att på förhand få ett skriftligt tillstånd av den ansvarige.

Vissa skyldigheter som tidigare har gällt för den personuppgiftsansvarige gäller nu även för biträdet, som kraven på att föra register över behandlingar, att säkerställa en lämplig säkerhetsnivå och att i vissa fall utse ett dataskyddsombud.

Även personuppgiftsbiträdet kan bli föremål för tillsyn eller administrativa sanktionsavgifter och bli skadeståndsansvarig. Den personuppgiftsansvarige och personuppgiftsbiträdet måste upprätta ett så kallat biträdesavtal. Avtalet ska bland annat innehålla instruktioner för hur personuppgiftsbiträdet får behandla personuppgifterna.

Underbiträde

Personuppgiftsbiträdet kan i sin tur anlita andra biträden, så kallade underbiträden, men endast om den personuppgiftsansvarige i förväg gett ett skriftligt tillstånd till detta.

Tillståndet kan gälla anlitande av ett visst underbiträde eller gälla generellt. Om ett biträde har ett generellt tillstånd måste ändå den personuppgiftsansvarige informeras.

Ett underbiträde omfattas av samma skyldigheter som det ursprungliga personuppgiftsbiträdet har mot den personuppgiftsansvarige enligt deras avtal.

Den personuppgiftsansvarige behöver även få reda på bland annat kontaktuppgifter till underbiträdet för att kunna utföra eventuella kontroller av hur underbiträdet lever upp till avtalet.

Använder ni Crona Lön som är en molntjänst, är ni som företag personuppgiftsansvarig, vi som förmedlare biträde och vår operatör som driftar tjänsten underbiträde.

Dataskyddsombud

Den som behandlar personuppgifter måste i vissa fall utse ett dataskyddsombud.

Ombudets roll är att kontrollera att dataskyddsförordningen följs genom att t.ex. utföra kontroller och informationsinsatser.

Ett Dataskyddsombud behöver endast utses i speciella fall och detta gäller inte för att man har ett personregister i Crona Lön.

Crona Lön och medarbetarens rättigheter

Supportdokument nr: LON0154
Programvara: Crona Lön, Modell: Alla

Bakgrund

I Crona Lön finns ett personregister med de medarbetare som har anställning på företaget eller är arvoderade som t.ex. styrelseledamöter. Alla personregister omfattas av dataskyddsförordningen (GDPR), så också det i Crona Lön. De medarbetare vars personuppgifter behandlas har ett antal rättigheter enligt denna förordning.

Dessa rättigheter innebär i korthet att de registrerade ska få information om när och hur deras personuppgifter behandlas och ha kontroll över sina egna uppgifter. Därför har de bland annat rätt att i vissa fall få sina uppgifter rättade, raderade eller blockerade, eller att få ut eller flytta sina uppgifter. De registrerades rättigheter har utökats, förstärkts och specificerats i dataskyddsförordningen jämfört med den tidigare personuppgiftslagen (PUL).

Rätt till information

Den registrerade har rätt att få information när dennes personuppgifter behandlas. Informationen ska tillhandahållas kostnadsfritt i en lättillgänglig, skriftlig form. Information om kontaktuppgifter till den personuppgiftsansvarige, den rättsliga grunden för behandlingen och ändamålet med behandlingen ska framgå.

Vid utskrift av *Personkort* kommer[1] all information om en anställda att redovisas utom dennes lönebesked, dessa har medarbetaren fått sedan tidigare, men kan givetvis skrivas ut på nytt.

Rätt till rättelse

Varje person har rätt att vända sig till företaget som behandlar personuppgifter för att få felaktiga uppgifter rättade. Det innebär också att den enskilde har rätt att komplettera med sådana personuppgifter som saknas och som är relevanta med hänsyn till ändamålet med behandlingen.

Att den som behandlar personuppgifter också själv måste se till att uppgifterna är korrekta och uppdaterade framgår redan av de grundläggande principerna i dataskyddsförordningen.

Avseende löneprogram ligger det givetvis i både företagets och den enskildes intresse att eventuella felaktigheter snarast korrigeras.

Begränsning av behandling

Enskilda har i vissa fall rätt att kräva att behandlingen av personuppgifter begränsas. Med begränsning menas att uppgifterna markeras så att dessa i framtiden endast får behandlas för vissa avgränsade syften.

Rätten till begränsning gäller bland annat när den registrerade anser att uppgifterna är felaktiga och begärt rättelse. I sådana fall kan den registrerade även begära att behandlingen av uppgifterna begränsas under tiden uppgifternas korrekthet utreds. Denna regel är inte tillämplig vid användning av Crona Lön eftersom syftet med personregistret vilar på rättslig förpliktelse.

Dataportabilitet

Den som har lämnat sina personuppgifter har också i vissa fall rätt att få ut och använda sina personuppgifter på annat håll. Den som har tagit emot personuppgifterna får inte hindra en sådan överflyttning av personuppgifter.

Förutsättningen är att personuppgifterna behandlas med stöd av ett samtycke eller för att uppfylla ett avtal med den registrerade och det gäller bara sådana uppgifter som den registrerade själv har lämnat.

Crona Lön behandlar som nämnts uppgifter grundat på rättslig förpliktelse så dataportabilitet berör inte löneprogrammet. Möjlighet finns dockatt via formatet PAXml att ta ut personuppgifterna om en person.

Rätt till radering - gallring

En medarbetar har rätt att vända sig till företaget och be att uppgifterna som avser denne raderas. Uppgifterna måste raderas i det fall att uppgifterna inte längre behövs för de ändamål som de samlades in eller behandlingen grundar sig på den enskildes samtycke och denne återkallar samtycket.

Nästan all information som sparas i Crona Lön är sådan som måste sparas, utifrån lagstiftning i minst sju år, ibland längre. Arbetsgivare också skyldig att kunna lämna ett arbetsgivarintyg som omfattar hela medarbetarens anställningstid om så begärs. De personuppgifter som bygger på rättslig förpliktelse behöver inte gallras endast de med vars ändamål blivit inaktuellt. En ny knapp[1], **[Gallra]**, gör just detta.

Gallra säkerhetskopior

För att en säkerhetskopia till Crona Lön ska vara meningsfull att återställa måste den vara aktuell. De får högst vara någon eller några månader gammal. Man får ta som regel att genomföra gallring direkt efter att en säkerhetskopia eventuellt har återställts. Äldre kopior raderas i sin helhet.

[1] Kommer att introduceras i god tid innan den 25:e maj 2018

Crona Lön och säkerheten

Supportdokument nr: LON0152
Programvara: Crona Lön, Modell: Alla

Bakgrund

Viktigt som användare av Crona Lön och andra applikationer i vårt sortiment är att veta hur säkra dessa applikationer är, inte minst med tanke på nya dataskyddsförordningen (GDPR) och personuppgifter.

Fysisk miljö

Crona Lön är en lokalt installerad applikation där både program och datainformationen normalt finns inom den egna arbetsplatsen.

På samma sätt som man skyddar annan egendom med lås och andra hinder ska detta givetvis också göras med den datainformation som sparas vid användning av löneprogrammet.

Det är alltid det enskilda företaget som har ansvaret avseende behörighet, åtkomlighet, virusskydd, etc. Hanterar man personregister ökar kravet på att ha låsbara skåp, avdelningar, etc. för att begränsa åtkomsten från obehöriga.

Det är den enskilde användaren som också får se till att obehöriga inte tar del av datainformation via utskrifter som t.ex. ligger länge i en gemensam skrivare, om någon står ”bakom ryggen” vid nyttjandet av Crona Lön, etc.

Företagets lokala nätverk måste skyddas från virus och obehörigas intrång.

Programmiljö

Crona Lön levereras med ett behörighetssystem för att kunna begränsa åtkomligheten inom det egna företaget. Vid leverans är det påslaget.

All datainformation i Crona Lön är krypterad och kan bara läsas av Crona Lön. Inga externa programvaror eller applikationer kan dekryptera informationen utan mycket stora ”hackerinsatser”. Saknas åtkomst till Crona Lön kan man heller inte komma åt informationen även om själva datafilerna ligger åtkomliga.

Säkerhetskopior

Crona Lön har ett avancerat system för att ta säkerhetskopior. Av just säkerhetsskäl bör tagna säkerhetskopior sparas separerat från den dator eller server från vilka de är tagna. Helst bör kopian sparas fysiskt på helt annan plats för att t.ex. klara brand och inbrott.

Givetvis är även säkerhetskopian krypterad. En säkerhetskopia kan dessutom endast återställas till den Crona Lön licens från vilken den är tagen[1] samt till vissa interna installationer hos oss på DataVara AB så att möjlighet finns för oss att lämna service och support[2]. Denna säkerhetsnivån är valbar.

DataVara AB erbjuder också en backup-funktion som innebär att vi hanterar kopiorna på en FTP server för att ytterligare stärka upp säkerheten.

Internet och e-post

I Crona Lön finns ett antal funktioner som innebär att programmet är uppkopplat mot Internet.

När man kör löneprogrammet finns en koppling till vår licensserver där Crona Lön kan läsa av ifall användaren har rätt att nyttja programmet och ifall det finns ett serviceavtal eller inte. Den information som hämtas från löneprogrammet till licenservern förutom dessa datum är antal aktiva företag och anställda, aldrig några identiteter.

Nyhetspanelen läser en eller flera RSS-kanaler (Rich Site Summary), ingen information lämnar löneprogrammet den vägen. Slutligen finns möjligheten att skicka e-post och digitala brev från Crona Lön. Inte heller här lämnar annan information än den som skickas från löneprogrammet i klartext, dvs. lönebesked och kontrolluppgifter.

För- och efterbehandlingssystem

Inget administrativ program kan längre finnas endast i sin egen värld. Kommunikation med andra applikationer är en förutsättning för ett bra administrativt hjälpmedel.

Ett löneprogram måste kunna lämna bokföringsdata till redovisningsprogrammet och kanske hämta in tidsstämplingar eller reseräkningar för vidare bearbetning. Dessa applikationer är ofta webbaserade, som vårt eget Crona Portal.

I Crona Lön finns möjlighet att skapa både import- och exportfiler samt möjligheten till API-koppling för att utbyta information till andra applikationer.

Exakt vilken information som ett externt försystem får tillgång till finns redovisat i speciella dokument som kan rekvireras från oss på DataVara AB.

Crona Lön som molntjänst

Crona Lön finns också som molntjänst i samarbete med en extern part. Närmare information om detta finns i supportdokumentet LON0159.

[1] Introduceras i god tid innan den 25:e maj 2018, [2] Support där vi tar del av kundens datainformation kräver att vi tecknar ettpersonuppgiftsbiträdesavtal

Crona Lön och känsliga uppgifter

Supportdokument nr: LON0153
Programvara: Crona Lön, Modell: Alla

Bakgrund

Vissa personuppgifter är till sin natur särskilt känsliga och har därför ett starkare skydd i dataskyddsförordningen (GDPR). Det handlar om så kallade känsliga personuppgifter som till exempel personuppgifter som avslöjar etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller uppgifter om hälsa och sexualliv, men även personuppgifter som rör lagöverträdelser som innefattar brott.

Utgångspunkten är att det är förbjudet att behandla sådana personuppgifter. Det finns dock flera undantag från förbudet. Även personnummer kan räknas till personuppgifter som är särskilt integritetskänsliga.

I Sverige arbetar för närvarande ett antal utredningar med att se över och ta fram kompletterande svensk lagstiftning när det gäller känsliga personuppgifter, uppgifter om lagöverträdelser och personnummer.

Känsliga personuppgifter

Med känsliga personuppgifter avses uppgifter om

- *ras eller etniskt ursprung*
- *politiska åsikter*
- *religiös eller filosofisk övertygelse*
- *medlemskap i en fackförening*
- *hälsa*
- *en persons sexualliv eller sexuella läggning*
- *genetiska uppgifter och*
- *biometriska uppgifter som entydigt identifierar en person.*

Genetiska och biometriska uppgifter liksom uppgifter om sexuell läggning är nya kategorier som lagts till som känsliga uppgifter i dataskyddsförordningen jämfört med personuppgiftslagen.

Genetiska uppgifter är personuppgifter som rör en persons nedärvda eller förvärvade genetiska kännetecken, vilka till exempel kan framgå av en dna-analys.

Biometriska uppgifter är personuppgifter som rör en persons fysiska, fysiologiska eller beteendemässiga kännetecken som erhållits genom en särskild teknisk behandling, till exempel fingeravtrycksuppgifter.

Person- och samordningsnummer

Dataskyddsförordningen ger medlemsstaterna möjlighet att bestämma särskilda villkor för när ett nationellt identifieringsnummer, det vill säga ett personnummer eller samordningsnummer, får behandlas.

Frågan om hur personnummer och samordningsnummer ska regleras i svensk rätt har hanterats av Dataskyddsutredningen som har föreslagit att sådana uppgifter ska få behandlas bara om det är klart motiverat med hänsyn till ändamålet med behandlingen, vikten av en säker identifiering eller något annat beaktansvärt skäl. Bestämmelsen motsvarar tidigare bestämmelse i personuppgiftslagen.

Precis som vid all personuppgiftsbehandling måste den som behandlar personuppgifter som rör personnummer och samordningsnummer alltid följa de grundläggande principerna för behandling av personuppgifter, ha en rättslig grund för behandlingen samt uppfylla övriga bestämmelser i dataskyddsförordningen och kompletterande bestämmelser i nationell rätt.

Crona Lön

Förvisso finns uppgift om person- och samordningsnummer i Crona Lön. En säker identifiering krävs gentemot myndigheter och andra organisationen som t.ex. Skatteverket, Försäkringskassa, pensionsstiftelser, etc.

Vidare finns information om en medarbetares medlemskap i en fackförening, detta för att kunna säkerställa rätt information till både medarbetaren och fackföreningen avseende t.ex. löner.

Även hälsa och därmed sjukfrånvaro betraktas som en känslig uppgift och självklart hanteras sjukfrånvaro av löneprogrammet. Ingen information om diagnoser eller behandlingar finns i Crona Lön. Inte heller några andra känsliga uppgifter enligt dataskyddsförordningen lista finns sparade i löneprogrammet.

Då känsliga uppgifter finns i Crona Lön krävs en god säkerhet, denna beskrivs i supportdokument LON0152.

Personuppgiftsansvarigs ansvar

Crona Lön begränsar givetvis inte möjligheten att i fritextfält och liknande skriva vadhelst man önskar. Det är då upp till den personuppgiftsansvarige att reglera detta och hantera det rättsligt.

Notera att som personuppgiftsansvarig har man det hela ansvaret, ett ansvar som inte kan delegeras.