Srf konsulterna

Branschkod GDPR

GDPR i Löneprocessen av Srf Lönsam

Branschkod GDPR
GDPR i Löneprocessen av Srf Lönsam

Uppdatering har skett fram till den 5 juni 2018.

Eventuella rättningar och kompletteringar kommer att publiceras på Srf konsulternas webbplats www.srfkonsult.se

Vi reserverar oss för eventuella feltryck

Srf konsulterna
Klarabergsgatan 33
111 21 Stockholm
Tel: 010-483 80 00
E-post: info@srfkonsult.se
Webbplats: www.srfkonsult.se

ISBN 978-91-983107-3-3

INNEHÅLL

BRANSCHÖVERENSKOMMELSE

GPPR förutsätter att all behandling av personuppgifter sker i enlighet med EU-förordningen-. Förordningen ger utrymme för branschorganisationer att närmare utforma uppförandekoder. I syfte att skapa en gemensam god sed för behandlingen av personuppgifter i lönebranschen har Srf Lönsam som en sammanslutning av företrädare för lönebranschen tagit fram denna branschkod i syfte att specificera tillämpningen av denna förordning.

Innehållet i vägledningen kommer att justeras allteftersom rättspraxis utvecklas.

GDPR, General Data Protection Regulation är den EU-förordning som utgör grunden för hur personuppgifter ska behandlas i Sverige tillsammans med den svenska dataskyddslagen. Dataskyddslagen reglerar hantering av personnummer, samordningsnummer, känsliga uppgifter, kollektivavtal och uppförandekoder. Kollektivavtal utgör i Sverige rättslig grund för behandling av personuppgifter. Personuppgifter behandlas i stor utsträckning i löneprocessen.

AVSIKTSFÖRKLARING

Branschkoden är riktlinjer för behandling av personuppgifter inom löneprocessen och baseras på gällande lagstiftning och föreskrifter i Sverige. Branschkoden innehåller en rad förtydliganden kring behandling av personuppgifter som stärker de registrerades integritet och underlättar den praktiska hanteringen av löneprocessen. Genom dessa riktlinjer skapas ett standardiserat sätt för den som är ansvarig för personuppgifter i löneprocessen för att uppfylla kraven kring personuppgiftsbehandling. De systemleverantör som väljer att följa branschkoden ges också vägledning om hur de ska uppfylla kraven i gällande lagstiftning genom Privacy by Default och Privacy by Design.

Branschkoden följer de grundläggande principerna inom integritetsskydd (GDPR artikel 5) om att t.ex. inte samla in mer information än vad som behövs, inte ha kvar informationen längre än nödvändigt och inte använda uppgifterna till något annat än vad som var syftet när de samlades in.

Branschkoden har tagits fram genom ett metodiskt arbete i Srf Lönsam där personuppgifterna i löneprocessen har granskats i detalj för att motivera de riktlinjer som fastställts.

Branschkoden förvaltas av Srf konsulterna i arbetsgruppen Srf Lönsam. Den kommer att uppdateras och utvecklas i Srf Lönsam för att följa kompletterande lagstiftning, riktlinjer, föreskrifter och prejudikat gällande personuppgiftsbehandling.

Omfattning

Denna branschkod är avgränsad till personuppgiftsbehandling kopplad till löneprocessen beskriven i SALK, Svensk standard för Auktoriserade Lönekonsulter.

Tvisteförfarande

Om det skulle uppstå en tvist kring behandling av personuppgifter mellan en registrerad och personuppgiftsansvarig så hänvisas till tillsynsmyndigheten.

Rättslig grund

Rättslig grund för behandling av personuppgifter utgörs av GDPR artikel 6.1 samt kollektivavtal enligt dataskyddslagen. I löneprocessen är de rättsliga grunderna för behandling av personuppgifter rättslig förpliktelse, avtal, kollektivavtal, intresseavvägning och allmän intresseavvägning.

Rättslig förpliktelse
Lönehantering innefattar personuppgiftsbehandling som berör många lagar. Inom arbetsrätten finns bland annat lagen om anställningsskydd (LAS) men även utifrån redovisningshänseende där löneunderlag utgör verifikationer och därmed omfattas av såväl bokföringslagen (BFL) som arkivlagen.

Avtal
Grunden för hantering av lön är anställningsavtalet. Avtalet är upprättat mellan två parter där den registrerade utgör den ena parten. Personuppgiftsbehandling krävs för att hantera de åtaganden som arbetsgivaren har utifrån anställningsavtalet för att betala ut lön.

Kollektivavtal
Arbetsgivare som är bundna av kollektivavtal har även ett antal åtaganden utifrån kollektivavtalen. En förutsättning för att kollektivavtal ska kunna utgöra rättslig grund för behandling av personuppgifter är att avtalet är tillgängligt för den registrerade. I annat fall är det grundläggande legalitetskravet i dataskyddsförordningen inte uppfyllt. En förutsättning är därmed även att både arbetsgivaren och den som utför löneprocessen, som behandlar personuppgifter, har tillgång till gällande kollektivavtal.

Intresseavvägning
I arbetsgivaransvaret ingår skyldigheter som gör att intresset av att behandla uppgifterna kan vara större än den anställdes intresse av att uppgifterna inte behandlas. Intresseavvägning innefattar personuppgiftsbehandling i enlighet med god sed på arbetsmarknaden. Det innebär således att behandling av personuppgifter för att planera, organisera, leda och följa upp arbetet är en intresseavvägning.

Allmän intresseavvägning
I arbetsgivaransvaret ingår att inkomma med underlag till myndigheter. Om denna behandling av personuppgifter är nödvändig för att utföra en uppgift av allmänt intresse så är den tillåten. Uppgiften ska regleras i EU-rätt eller svensk rätt och uppgiften följer av lag eller annan författning av ett beslut som meddelats med stöd av lag eller annan författning, registerförfattningar. För behandling av personuppgifter inom löneprocessen innebär det även att organisationer som behandlar personuppgifter som ett led i myndighetsutövning kan ha allmän intresseavvägning som rättslig grund för behandling av personuppgifter.

Samtycke
För behandling av personuppgifter som inte har rättslig förpliktelse, avtal, intresseavvägning, allmän intresseavvägning eller kollektivavtal som rättslig grund krävs ett godkännande av den anställde i form av samtycke. Samtycke är mycket sällan rättslig grund för behandling av personuppgifter på arbetsplatsen, såvida arbetstagarna inte kan säga nej utan att detta får negativa konsekvenser. Om samtycke används måste det vara frivilligt, särskilt, informerat och en otvetydig viljeyttring. Samtycket ska vara individuellt men en facklig organisation kan samla in samtycken från varje enskild medlem och lämnar dessa vidare till arbetsgivaren.

Beskrivning av kategorierna av registrerade

Branschkoden omfattar behandling av registrerade för att utföra lönebearbetning. Inom löneprocessen behandlas blivande anställda, anställda, tidigare anställda, uppdragstagare samt andra personer som av någon anledning får utbetalning från ett lönesystem. Sammantaget kan dessa kategorier benämnas betalningsmottagare. Det finns även en kategori av registrerade som används i upplysningssyfte, exempelvis närstående, till vilka arbetsgivaren inte har någon relation men där uppgifterna krävs för att säkerställa att kriterier för t ex föräldraledighet uppfylls.

Blivande anställda

Arbetsgivaren får endast samla in och behandla arbetssökandes personuppgifter i den mån det är nödvändigt och relevant för utförandet av det arbete som personen söker. Det ska finnas ett berättigat intresse. Om det i verksamhetens löneprocess ingår att lägga upp personuppgifter i system innan anställning är påbörjad så ska de uppgifter som samlas in under rekryteringsprocessen raderas så fort det står klart att den personen inte kommer att erbjudas anställning eller tackar nej till erbjudandet. Det kan hända att det i ansökningshandlingar förekommer personuppgifter som kräver samtycke för att behandlas, t ex vissa kategorier av känsliga uppgifter. Samtycke kan därför vara ett bättre alternativ här. Rättslig grund är under rekryteringsprocessen samtycke.

Anställda

Arbetsgivaren måste behandla personuppgifter för att kunna uppfylla överenskommelser enligt avtal och lag. Rättslig grund för behandling av personuppgifter varierar beroende på vilken typ av personuppgift det gäller.

Tidigare anställda

Arbetsgivaren måste behandla personuppgifter för att kunna uppfylla överenskommelser enligt avtal och lag. Rättslig grund för behandling av personuppgifter varierar beroende på vilken typ av personuppgift det gäller. Arbetsgivaren har rätt att spara viss information om arbetstagaren; anledning till uppsägning, intyg, betyg och andra omdömen angående anställningen som tillställts arbetstagaren före och efter det att anställningen avslutats.

Uppdragstagare

Villkoren för uppdragstagare kan variera utifrån verksamhet och uppdragsgivare, i detta fall motsvarande anställda. Rättslig grund för behandling av personuppgifter varierar beroende på vilken typ av personuppgift det gäller.

Närstående

Personuppgiftsbehandling av uppgifter avseende närstående med syfte att beakta regler om sociala förmåner och rättigheter ska framgå av lag eller krav från myndighet. Anhörigas namn och kontaktuppgifter kan registreras utifrån intresseavvägning som rättslig grund. Samtycke behöver inte inhämtas från de anhöriga men de anställda måste informera sina anhöriga om att uppgifterna är utlämnade.

Behandling av särskilda kategorier av uppgifter

Lönehantering innefattar en hel del särskilda kategorier av uppgifter. I enlighet med GDPR artikel 9.2 är behandlingen ofta nödvändig för att den personuppgiftsansvarige eller den registrerade ska kunna fullgöra sina skyldigheter och utöva sina särskilda rättigheter inom arbetsrätten. Behandlingen kan i löneprocessen vara nödvändig för att skydda den registrerades eller någon annan fysisk persons grundläggande intresse. Behandlingen kan vara nödvändig för att fastställa, göra gällande eller försvara rättsliga anspråk eller som en del av domstolarnas dömande verksamhet. Behandling kan vara nödvändig för att kunna fullgöra sina skyldigheter eller utöva sina rättigheter gentemot sina arbetstagare och deras fackliga organisationer. Behandlingen kan vara nödvändig av skäl som hör samman med förebyggande hälso- och sjukvård och yrkesmedicin, bedömningen av en arbetstagares arbetskapacitet och medicinska diagnoser. Det finns därmed anledning till behandling av särskilda kategorier av uppgifter i löneprocessen. Det medför att behandling av personuppgifter inom löneprocessen kräver särskild aktsamhet gällande åtkomst och behörighet. Det åligger den personuppgiftsansvarige, som ofta även är ytterst ansvarig för lönehanteringen, att säkerställa en hög säkerhet kring åtkomst och ett tydligt behörighetssystem med dokumenterade rutiner för att anses följa denna branschkod.

Personnummer

Personnummer och samordningsnummer får behandlas utan samtycke endast när det är klart motiverat med hänsyn till ändamålet med behandlingen, vikten av en säker identifiering eller något annat beaktansvärt skäl. I löneprocessen kan behandling av personuppgifter kräva att personnummer används för identifiering mot t ex myndigheter. Personnummer rekommenderas inte att användas som anställningsid.

Uppgifter om barn

Dataskyddslagen har en tydlig gräns för när en registrerad anses vara tillräckligt gammal för att ingå samtycke enligt GDPR. Den gränsen är i Sverige 13 år vilket sammanfaller med när man vanligtvis får börja förvärvsarbeta. Det innebär att barn under 13 år inte kommer att vara mottagare av lön förutom i särskilt ovanliga fall. Däremot så används barns personuppgifter för att styrka den registrerades rättigheter enligt rättslig grund som rättslig förpliktelse, avtal och intresseavvägning.

Behandling av personuppgifter gällande barn

Inom löneprocessen kan behandling av uppgifter om barn ingå för att uppfylla krav från Försäkringskassan kopplat till föräldraförsäkring med rättslig förpliktelse som rättslig grund samt, i förekommande fall rapportering av uppgifter för tjänstepension och efterlevnadsskydd med kollektivavtal som rättslig grund. De personuppgifter som kan komma ifråga är barnets födelsedatum med eventuellt namn och detta ska behandlas med särskild försiktighet.

Särskilt om behandling av skyddade personuppgifter

Det finns olika typer av skyddade personuppgifter. Skatteverket kan besluta om sekretessmarkering och kvarskrivning. Sekretessmarkering innebär att Skatteverket för in en markering om sekretess i folkbokföringen varvid myndigheter inte får lämna ut uppgifterna utan kontroll och tillstånd. Kvarskrivning innebär att den registrerades folkbokföringsadress tas bort och den enskilde registreras som ”på kommunen skriven” i den tidigare folkbokföringsorten. Skattekontorets adress anges som en särskild postadress och posten vidarebefordras genom Skatteverkets försorg. Ytterligare en typ av skyddade personuppgifter är fingerade personuppgifter. Den enskilde får i dessa fall genom polisen en helt ny identitet; nytt personnamn och personnummer. I löneprocessen hanteras registrerade med skyddade personuppgifter med höga krav på begränsad åtkomst och sekretess.

Kategori av personuppgifter

Inom löneprocessen hanteras personuppgifter, och där till hörande anhöriguppgifter, skatteuppgift, anställningsuppgifter utifrån anställningsavtalet, lön, förmån, kontrolluppgifter, individuppgifter till arbetsgivardeklaration, lönetillägg, underlag för pension och försäkringar, regelverk, divisorer, lönetransaktioner, kontering, finansiellt underlag, semester, hälsa och statistik. Dessutom hanteras personuppgifter i inrapportering och extern rapportering. I denna branschkod identifieras personuppgifter i löneprocessen, kategoriseras och beskrivs utifrån vilken rättslig grund som personuppgifter behandlas. Många uppgifter används i flera av kategorierna och kan behandlas utifrån flera rättsliga grunder.

Inkomstuppgift

Inkomstuppgifter är de uppgifter som ligger till grund för beräkning och rapportering av lön.
Rättslig grund för behandling av personuppgifter är rättslig förpliktelse.
Exempel: uppgift om månadslön, timlön, ersättningar, underlag för arbetsgivardeklaration och kontrolluppgifter

Avtalsrelaterade uppgifter

Avtalsrelaterade uppgifter är uppgifter som utgör förutsättningar i anställnings- eller kollektivavtal
Rättslig grund är kollektivavtal.
Exempel: sysselsättningsgrad, semesterrätt, facklig tillhörighet

Finansiellt underlag

Uppgifter som utgör finansiellt underlag och verifikat. Rättslig grund är rättslig förpliktelse.
Exempel: bokföringsunderlag, semesterlöneskuld

Tjänsteuppgift

Uppgifter som anger förutsättningar för tjänst/befattning. Rättslig grund är avtal (anställningsavtal).
Exempel: befattningsbenämning, månadslön

Statistik

Uppgifter som används för att sammanställa statistik. Rättslig grund är intresseavvägning.
Exempel: lönetransaktioner

Kontaktuppgift betalningsmottagare

Uppgifter som används för att kunna kommunicera med betalningsmottagare. Rättslig grund är rättslig förpliktelse.
Exempel: adress, födelsedatum, namn och telefonnummer

Kontaktuppgift anhörig

Uppgifter som används för att kunna kommunicera med anhörig. Rättslig grund är intresseavvägning.
Exempel: adress, födelsedatum, namn och telefonnummer

TEKNISKA OCH ORGANISATORISKA ÅTGÄRDER

Enligt den nya dataskyddsförordningen har samtliga personuppgiftsansvariga ett ansvar att se till att det finns ett fullgott dataskydd. Personuppgiftsansvariga har en skyldighet att genomföra tekniska och organisatoriska åtgärder för att kunna efterfölja dataskyddsförordningen. Inom löneprocessen utgör IT-system och strukturerat material primärt platsen för behandling av personuppgifter, men mycket av underlag och kommunikation finns även i ostrukturerat material såväl i data som i pappersformat. Att följa denna branschkod innebär att säkerställa korrekt hantering i alla led.

INVENTERING LÖNEPROCESSEN

I löneprocessen bör alltid de grundläggande dataskyddsprinciperna följas, oavsett vilka system och vilken teknik som används. Uppgifterna ska behandlas för specificerade och berättigade ändamål som är proportionerliga och nödvändiga för löneprocessen. En förutsättning för en kvalitetssäkrad löneprocess är att uppgifterna är adekvata och relevanta. Att följa denna branschkod innebär att behandla de personuppgifter som är nödvändiga för löneprocessen och iaktta försiktighet kring insamlande av personuppgifter. Det innebär även att inte spara mer uppgifter än vad som är nödvändigt med hänsyn till det berättigade ändamålet, se till att de registrerade kan utöva sina rättigheter, däribland rätten att få tillgång till och, i förekommande fall, erhålla rättelse, radering eller blockering av personuppgifter, se till att uppgifterna är korrekta och inte behålla dem längre än nödvändigt, och vidta alla nödvändiga åtgärder för att skydda uppgifterna mot obehörig åtkomst och se till att personalen är tillräckligt medveten om sina skyldigheter när det gäller uppgiftsskydd.

Registerförteckning

Löneprocessen kan bestå av flera olika stödsystem som är mer eller mindre integrerade. Att följa denna branschkod innebär att ha en uppdaterad processkarta med registerförteckning över i vilka sammanhang utbyte av information av löneuppgifter sker.
Löneprocessen innebär behandling av personuppgifter som kan omfatta särskilda kategorier enligt GDPR artikel 9 och därför bör en registerförteckning finnas med följande uppgifter:

- Namn och kontaktuppgifter för den personuppgiftsansvarige, den personuppgiftsansvariges företrädare samt eventuellt dataskyddsombud.
- Ändamålen med behandlingen vilket är att utföra löneprocessen enligt de överenskommelser och förpliktelser som gäller enligt lag och avtal.
- En beskrivning av de kategorier av registrerade och de kategorier av personuppgifter som är betalningsmottagare enligt denna branschkodsbeskrivning och de personuppgifter som krävs för att utföra löneprocessen enligt det som kategoriserats enligt denna branschkod.
- De kategorier av mottagare till vilka personuppgifterna har lämnats eller ska lämnas ut. Inom löneprocessen gjord inventering enligt denna branschkod tydliggöra att personuppgifter skickas till SCB, Skatteverket, försäkrings- och pensionsförmedlare, Försäkringskassan, Kronofogden m.fl. med rättslig grund enligt avtal och rättslig förpliktelse.
- Om det sker överföringar av personuppgifter till ett tredjeland, dvs ett land som inte är medlem i EU/EES eller en internationell organisation ska det framgå och det måste baseras på rättslig grund. Arbetstagarnas personuppgifter får endast överföras till andra länder som garanterar en adekvat skyddsnivå, överföringen omfattas av lämpliga skyddsåtgärder, det finns bindande företagsbestämmelser. Överföring utöver detta måste grunda sig på en internationell överenskommelse utan att detta påverkar andra grunder för överföring till tredjeland. Det finns även särskilda undantag enligt GDPR artikel 49. För dessa undantag krävs kontakt med Datainspektionen innan överföring initieras.
- Gallrings- och arkiveringsregler som finns definierade i branschkoden.
- Om möjligt, en allmän beskrivning av tekniska och organisatoriska säkerhetsåtgärder.

Systemkarta

En förteckning över antalet system med integrationspunkter, det innebär alla system som är kopplade till löneprocessen. Molntjänster kräver särskild hantering och förutsättningarna kan variera. För att kunna upprätthålla kvalitet utifrån branschkoden är det viktigt att ha en bra förvaltning av system. Ytterligare stöd för den hanteringen finns i SALK, Svensk standard för Auktoriserade Lönekonsulter.

Behörigheter

För att kunna skydda personuppgifter krävs att endast de med behörighet har åtkomst. Behörigheterna ska vara rollrelaterade och uppdateras kontinuerligt utifrån förändringar i organisationen. De olika behörighetsnivåerna ska dokumenteras liksom rutiner för uppdatering vid förändringar.

Inventering av ostrukturerat och strukturerat material

I löneprocessen behandlas personuppgifter (tidrapporter, utläggsunderlag, läkarintyg, skatteunderlag etc.) både som strukturerat (t ex lönesystem) som ostrukturerat material (t ex e-post). Behandlingen ska vara kartlagd och behörighetsstyrd. Personuppgifter som inkommer och utgör underlag till löneprocessen bör i den mån det är möjligt hanteras via webbportal, krypterat format eller ärendehanteringssystem. Det ska finnas allmänna gallringsrutiner för e-post.

Minimera mängden personuppgifter

Branschkoden innebär att begränsa sig till uppgifter som endast indirekt pekar ut en individ i den mån det är möjligt. Det gäller att i kommunikation begränsa de uppgifter som är känsliga och att ersätta namn med anställningsid som är exempel på godtagbara pseudonymer. Tillgång till de uppgifter som förutsätter löneprocessens arbetsmoment ska styras av tydliga behörigheter för att minska åtkomst. Löneprocessen förutsätter hantering av personnummer. Rättslig grund är rättslig förpliktelse. Den legala grunden till detta ska dokumenteras enligt GDPR artikel 87 och §13 dataskyddslagen.

Konsekvensbedömning

Konsekvensbedömning är en process för att skapa och påvisa efterlevnad av GDPR utifrån risken när behandling av personuppgifter sannolikt leder till en hög risk för fysiska personers rättigheter och friheter. I löneprocessen används vanligtvis ett lönesystem. Personuppgiftsansvariga är skyldiga att kontinuerligt bedöma den risk som uppkommer vid behandling av personuppgifter. För en leverantör som följer branschkoden kan det medföra att krav på konsekvensbedömning är uppfyllt gällande de uppgifter som finns i systemet. En konsekvensbedömning innebär att ha en beskrivning av den planerade behandlingen och behandlingens syften. Det ska göras en bedömning av behovet och proportionalitet hos behandlingen i förhållande till syftet/syftena. Den personuppgiftsansvarige ska utvärdera och uppdatera bedömningen av riskerna för de fysiska personernas rättigheter och friheter. Detta ska göras med åtgärder som planeras för att hantera eventuella risker med skyddsåtgärder, säkerhetsåtgärder och rutiner för att säkerställa skyddet av personuppgifter. I enlighet med GDPR innebär branschkoden att tillgång och åtkomst till personuppgifter är begränsad utifrån förutsättningarna i Privacy by Default och Privacy by Design som de systemleverantörer som följer denna branschkod stödjer.

Personuppgiftsbiträden

Ansvaret för att behandlingen av personuppgifter i löneprocessen sker i enlighet med gällande lagstiftning är alltid den personuppgiftsansvarige. Om löneprocessen innefattar personuppgiftsbiträde som behandlar personuppgifter för den personuppgiftsansvariges räkning krävs att det finns reglerat på vilket sätt och i vilken omfattning. För de företag som outsourcar hela eller delar av löneprocessen eller använder molntjänster krävs i de allra flesta fall ett personuppgiftsbiträdesavtal. Det är den personuppgiftsansvariga som ska säkerställa att det finns ett personuppgiftsbiträdesavtal enligt GDPR artikel 28.

Dataskyddsombud

Dataskyddsombud ska utses hos de företag där behandling av lön utgör kärnverksamheten. Företag som omfattas av krav på dataskyddsombud har anställda vars personuppgifter ingår i löneprocessen och därmed kontrolleras av ett dataskyddsombud. Myndigheter och offentliga organ måste ha ett dataskyddsombud oavsett vilka uppgifter de behandlar. Srf Lönsam rekommenderar att leverantörer som behandlar personuppgifter i egenskap av personuppgiftsbiträde bör ha ett internt eller externt dataskyddsombud.

INFORMATION TILL DEN REGISTRERADE

Den svenska arbetsmarknadsmodellen ställer höga krav på informationsutbyte för de företag som har kollektivavtal gällande förutsättningar och förändringar i organisationen. GDPR medför en stärkt rätt för den registrerade när det gäller tillgång och hantering av de egna personuppgifterna. GDPR innebär en skyldighet för den personuppgiftsansvariga att på ett transparent och tydligt sätt visa vilka personuppgifter som behandlas, till vad och hur länge. Den personuppgiftsansvarige ska därför informera om vilka personuppgifter som hanteras i löneprocessen, vilka rapporter som skickas till externa mottagare samt vilka arkiverings- och gallringsregler som finns för att uppfylla rättsliga, kollektivavtalskopplade och avtalsenliga förpliktelser. Informationen delges i samband med att personuppgifter mottas från den registrerade av den personuppgiftsansvarige. Vid förändringar av behandling/rapportering ska detta delges de registrerade på ett tydligt sätt.

Tillgång till personuppgifter

Enligt GDPR föreligger en rätt för den registrerade att begära tillgång till sina personuppgifter, rätt till rättelse, radering, begränsning av sina personuppgifter eller att invända mot behandling samt rätten till dataportabilitet. Den registrerade har även rätt att inge klagomål till tillsynsmyndigheten. Inom löneprocessen är behandling av personuppgifter en förutsättning för att tillmötesgå den registrerades rättigheter som betalningsmottagare/anställd utifrån kraven i GDPR. Denna branschkod tydliggör vad som är gällande i de fall som är specifika för löneprocessen.

Rätten till tillgång

För att upprätthålla de åtaganden som den personuppgiftsansvarige har i form av utbetalare och/eller arbetsgivare måste den registrerade inkomma med uppgifter såsom personnummer, kontaktuppgifter och skatteuppgifter. De uppgifter som tillkommer för att kunna utföra löneprocessen baserar sig på ett anställningsavtal. Den registrerade har genom ett registerutdrag bland annat rätt att få kontaktuppgifter till den personuppgiftsansvarige, information om den rättsliga grunden för behandlingen och ändamålet med behandlingen. Denna branschkod kan användas som en kompletterande information men personuppgiftsansvarig måste kunna påvisa personuppgiftsbehandlingen utifrån den egna löneprocessen. Viktigt är att den registrerade kan ta del av vart information med personuppgifter skickas utanför organisationen, t ex statistik till SCB, tjänstepensionsrapportering och arbetsgivardeklaration på individnivå (AGI) till Skatteverket. Om personuppgiftsbehandlingen innefattar överförande av data till tredjeland bör särskilda åtgärder vidtas och den registrerade informeras.

Registerutdrag

Den registrerade kan kräva ett registerutdrag. Ett registerutdrag ska innehålla alla de personuppgifter som rör personen som sökt registerutdrag, varifrån dessa uppgifter kommer, vad som är ändamålet med behandlingen och till vilka mottagare eller kategorier av mottagare uppgifterna lämnas ut. Ett registerutdrag ur ett lönesystem motsvarar personkort/anställningsavtal med nuvarande synliga värden. Lönetransaktioner och annan behandling av data för att utföra löneprocessen ingår inte i det som motsvarar ett registerutdrag. Registerutdrag ska levereras enkelt och lättförståeligt i skrift. Om en begäran om registerutdrag inkommer i elektronisk form har den registrerade rätt att få utdraget levererat i elektronisk form.

Exempel på vad ett registerutdrag bör innehålla för uppgifter:

- Namn
- Personnummer
- Adress
- Semesterrätt
- Semesteravtal
- Anhörig/närståendes kontaktuppgifter
- Information kring barn
- Skattetabell
- Jämkning
- Förmåner
- Kompsaldo
- Schema
- Anteckningar
- Tillägg/avdrag på lön (pågående)
- Månadslön/timlön

Rätten till att få personuppgifter rättade

Korrekta personuppgifter är en förutsättning för att löneprocessen ska vara kvalitetssäkrad. Att den registrerade inkommer med rättade uppgifter är välkommet och ska åtgärdas omgående.

Rätten till att få personuppgifter raderade

Personuppgifter som behandlas i löneprocessen utgör underlag och verifikat som kan behövas för att styrka utfall i händelse av revision, tvist och kontroll att rättsliga åtagande är uppfyllda. När väl personuppgifter finns registrerade och är kopplade till lönetransaktioner i löneprocessen kan den registrerade därför inte hävda rätten till att få personuppgifter som krävs för att styrka förutsättningar för en given lönehändelse eller rapportering raderade.

Dataportabilitet

Rätten till dataportabilitet syftar till att ge de registrerade mer inflytande över sina egna personuppgifter, eftersom den gör det lättare att flytta, kopiera eller överföra personuppgifter från en IT-miljö till en annan. Dataportabilitet innebär att den registrerade kan ha rätt att få ut en del av sina personuppgifter, lagra dessa uppgifter för personligt bruk och även överföra personuppgifter från en personuppgiftsansvarig till en annan. Dataportabilitet innefattar de personuppgifter som rör den registrerade och som den registrerade själv har tillhandahållit en personuppgiftsansvarig för behandling och sådana uppgifter som är ett resultat av detta tillhandahållande. När det gäller uppgifter som har skapats av den personuppgiftsansvarige som utgör underlag såsom

lönetransaktioner är dessa ett led i behandlingen inom ramen för löneprocessen och inget som den anställde själv har tillhandahållit. De har inte tillhandahållits av den registrerade utan skapas av den personuppgiftsansvarige. Sådana personuppgifter likväl som uppgifter som har skapats genom kategorisering av användare eller genom profilering är uppgifter som är härledda eller avledda från de personuppgifter som den registrerade har tillhandahållit. De omfattas därför inte av rätten till dataportabilitet. Dataportabilitet är därmed inte tillämplig för uppgifter som har skapats i löneprocessen. GDPR:s krav på dataportabiliteten medför inte utökade krav på att lagra uppgifter under längre tid än de lagringstider som annars gäller, bara för att eventuellt tillmötesgå en framtida begäran om dataportabilitet. Dataportabilitet leder inte automatiskt till att uppgifter raderas från den personuppgiftsansvariges system, och påverkar inte den ursprungliga lagringsperioden för de uppgifter som har överförts.

FÖRETAGSPOLICYER

Personuppgiftsansvarig har ett långt gående ansvar utifrån GDPR men även som arbetsgivare. Behandling av personuppgifter förutsätter transparens och tydlighet. För att detta ska uppnås bör det finnas tydliga företagspolicyer för vilka, på vilket sätt och hur länge personuppgifter sparas. Kraven på att minimera mängden personuppgifter medför en begränsning i hur långtgående den personuppgiftsansvariges åtaganden kan bli. Det finns därmed även ett ansvar för den registrerade att ta till sig den information som den personuppgiftsansvarige delger. Arbetsgivaren ska ha en rutin för hur information om behandlingen av personuppgifter ska lämnas till den registrerade. Informationen bör lämnas skriftligen och informationstexter ska ses över och revideras kontinuerligt.

Information kan lämnas som en bilaga till anställnings/uppdragsavtal eller via företagets hemsida. En hänvisning till hemsidan kan lämnas i avtal och liknande. Informationen ska vara lätt att hitta på hemsidan och utbetalaren ska tillhandahålla papperskopior på informationen om en registrerad begär det. Om informationen ändras bör betalningsmottagare uppmärksammas på det genom e-post eller motsvarande. Det är möjligt att lämna informationen om att det har skett förändringar i hanteringen av personuppgifter genom att hänvisa till en hemsida.

GALLRING, ARKIVERING OCH BEVARANDE

GDPR innebär en skyldighet att på ett transparent och tydligt sätt visa hur personuppgifter sparas och varför. I löneprocessen är det den rättsliga grunden för behandling av personuppgifter som avgör under vilken period som personuppgifterna kommer att lagras eller om detta inte är möjligt, kriterier för att fastställa denna period.

Inom löneprocessen finns följande kategorier av personuppgifter:

Inkomstuppgift - Uppgifter som ligger till grund för beräkning av lön

Uppgifter som ingår i denna kategori måste sparas så länge det finns en möjlighet att de kan behövas för att styrka en historisk inkomst. Det innebär flera år efter anställningens slut för att kunna hantera förutsättningar inom arbetsrätten. Rättslig grund är rättslig förpliktelse.

Avtalsrelaterat - Förutsättningar i anställnings - eller kollektivavtal

Uppgifter som ingår i denna kategori måste sparas så länge det finns en möjlighet att de kan behövas för att styrka förutsättningar i anställningsförhållandet i relation till kollektivavtal. Det innebär flera år efter anställningens slut, till dess att den registrerade avlider eller uppnår pensionsålder. Rättslig grund är kollektivavtal.

AGI/KU - Underlag arbetsgivardeklaration/kontrolluppgift

Uppgifter som ingår i denna kategori måste sparas så länge som de behövs för att styrka rapporteringen till Skatteverket, dvs i minst sju år. Rättslig grund är rättslig förpliktelse.

Finansiellt underlag - Uppgifter som utgör finansiellt underlag

Dessa uppgifter faller under bokföringslagen, arkivlagen, preskriptionslagen och penningtvättslagen och ska därmed följa tillämplig lagstiftning. Rättslig grund är rättslig förpliktelse.

Tjänsteuppgift - Uppgifter som anger förutsättningar för tjänst/befattning

Uppgifter måste sparas så länge det finns en möjlighet att de kan behövas för att styrka förutsättningarna i en anställning. Rättslig grund är avtal (anställningsavtal).

Statistik - Uppgift för statistikunderlag

Uppgifter som används för att sammanställa statistik. Rättslig grund är allmänt intresse.

Kontaktuppgift - Uppgifter till betalningsmottagare alternativ anhörig

Uppgifter ska sparas så länge det finns rättlig grund för att kunna kommunicera med betalningsmottagare alternativt anhörig. Rättslig grund är intresseavvägning.

Minnesanteckningar

I samband med löneprocessen kan det behöva göras minnesanteckningar för t ex en justering av en lön. Sådana uppgifter kan bevaras på motsvarande sätt som övriga underlag för lön för att styrka en utbetalning. Rätten att få ut minnesanteckningar finns kopplat till registerutdraget.

Arkivering

En gallrings- och arkiveringsplan ska finnas för personuppgifter. I och med att flera av de kategorier av personuppgifter används för att uppfylla flera rättsliga grunder och det inte går att bryta ut särskild information så ska personuppgifter som behandlas i löneprocessen arkiveras i tio år för att därefter gallras utifrån gällande preskriptionslag som ställer längst krav på bevarande av uppgifter. Det gäller för samtliga personuppgifter med följande tillägg och undantag:

Gallring undantag från 10-årsregeln

Det finns särskilda uppgifter där det inte finns rättslig grund för bevarande enligt 10-årsregeln. Dessa särskilda uppgifter kan variera beroende på verksamhet.

Tillfälliga åligganden

Personuppgiftsansvariga behandlar personuppgifter för tillfälliga åligganden i löneprocessen. Det finns flera exempel. I samband med sjukdom hanteras läkarutlåtanden, även kallat läkarintyg, för att styrka rättigheter. Rättslig grund för behandling av läkarutlåtanden är rättslig förpliktelse och den personuppgiftsansvarige ska endast ta emot sidan två. Läkarutlåtande ska gallras när personen tillfrisknat och alltså åter börjat arbeta eller det pågår en aktiv rehabiliteringsprocess med reservation för återinsjuknade.

Fria textfält

I lönesystemen finns ofta en möjlighet att föra in uppgifter som inte är förutbestämda i så kallade fria textfält. Det är den personuppgiftsansvariga som ansvarar för att dessa fält inte används för att notera uppgifter som strider mot GDPR.

Omedelbart vid slutlön

- Närstående/anhörigs kontaktuppgifter

Det finns rättslig grund för behandling av närstående/anhörigs kontaktuppgifter så länge betalningsmottagare har ett pågående avtal. När det avtalet upphör så upphör även den rättsliga grunden för behandling.

- Facklig tillhörighet

Det finns rättslig grund för hantering av facklig tillhörighet som anses ingå i särskild kategori av personuppgift utifrån kollektivavtal som förutsätter behandling av uppgiften. När betalningsmottagaren inte längre omfattas av kollektivavtalet upphör även den rättsliga grunden för behandling.

- Bankkontonummer

Det finns rättslig grund för att behandla bankkontonummer så länge betalningsmottagare har ett pågående avtal. När det avtalet upphör och sista löneutbetalningen är gjord så upphör även den rättsliga grunden för behandling.

Vid årsskiftesrutin på avslutade anställda inom ett kalenderår från avgångsdatum

- Kontakt/adressuppgifter till anställd

Det finns rättslig grund för att behandla kontakt/adressuppgifter under ett år efter att betalningsmottagaren har avslutat sitt uppdrag hos den personuppgiftsansvarige. Detta eftersom det utifrån från en intresseavvägning kan finnas behov av att nå betalningsmottagaren om t ex en felaktig lön har utbetalats.

Övriga rekommendationer

Branschkoden rekommenderar att en årsskiftesrutin införs för uttag av underlag för pensionsrapportering som sparas hos arbetsgivare livslångt bland personalakter istället för att spara uppgifter i lönesystem. Underlaget bör innehålla information kring pensionsgrundande inkomst, personnummer, personalkategori och andra uppgifter som rapporterats till pensionsinstitut exempelvis frånvaro samt pensionsavtal.

Branschkoden rekommenderar att arbetsgivarintyg tas fram vid varje slutlönsberäkning och sparas hos arbetsgivare bland personalakter istället för att spara uppgifter i lönesystemet.

CENTRALA BEGREPP

Dataskyddsförordningen har flera begrepp som är viktiga att förstå för att kunna kontrollera att de krav som ställs upp i GDPR-förordningen efterföljs.

ADEKVAT SKYDDSNIVÅ

Riktlinjer för vad man måste tänka på när man bedömer skyddsnivån för personuppgifter mellan länder.

DATAINSPEKTIONEN/INTEGRITETSSKYDDSMYNDIGHETEN/DATASKYDDSMYNDIGHETEN

Myndighet som arbetar för att säkra den enskilda individens rätt till integritet i samhället. Tillsynsmyndighet för att övervaka så att de som behandlar personuppgifter följer dataskyddsförordningen. Står under namnbyte från Datainspektionen till något av förslagen Integritetsskyddsmyndigheten eller Dataskyddsmyndigheten.

DATA PROCESSING OFFICER (DPO)

Engelska benämningen av dataskyddsombud

DATASKYDDSDIREKTIVET

EU-direktiv från 1995 som personuppgiftslagen härrör från.

DATASKYDDSFÖRORDNINGEN

Dataskyddsförordningen, eller GDPR som den också kallas, innehåller regler om hur man får behandla personuppgifter. Förordningen gäller från 25 maj 2018 och ersätter personuppgiftslagen. (PuL).

DATASKYDDSLAGEN

Ny nationell reglering som på ett generellt plan kompletterar dataskyddsförordningen (GDPR).

DATASKYDDSOMBUD

Oberoende person utan ledande ställning inom eller utanför företag med krav på dataskyddsombud som säkerställer korrekt personuppgiftshantering och är kontaktperson för t ex myndigheter.

DIREKTIV

Beslut från EU som sätter upp vilka mål medlemsländerna ska uppnå, men lämnar åt medlemsländerna att avgöra exakt hur.

EUROPEISKA DATASKYDDSSTYRELSEN

Representanter från EU:s nationella tillsynsmyndigheter med uppdrag att bidra till en enhetlig tillämpning av förordningen (European Data Protection Board, EDPB).

EU:S ALLMÄNNA DATASKYDDSFÖRORDNING

Annan benämning på Dataskyddsförordningen.

EU:S DATASKYDDSREFORM

Nytt regelverk som EU har beslutat för behandling av personuppgifter. Dataskyddsreformen består av två delar; GDPR och ett direktiv om personuppgiftsbehandling som utförs av brottsbekämpande verksamheter.

EXTRA SKYDDSVÄRDA PERSONUPPGIFTER

Extra skyddsvärda uppgifter är inte definierade i GDPR men är de uppgifter som anses vara särskilt viktiga att skydda t ex: personnummer, information som omfattas av sekretess eller tystnadsplikt, vissa uppgifter om ekonomiska förhållanden, omdömen och värderingar av en person såsom social förmåga, inlärningsförmåga och liknande, provresultat, resultat av personlighetstester och annan information som ligger nära den privata sfären.

Det finns inget förbud mot att behandla dessa, men de ska hanteras med extra försiktighet. Förordningen kräver att man vidtar säkerhetsåtgärder som reflekterar uppgifternas art och risken som behandlingen medför för den registrerade.

FÖRORDNING

Beslut från EU som gäller direkt och likadant i alla medlemsländer som en del av den nationella lagstiftningen.

GENERAL DATA PROTECTION REGULATION (GDPR)

GDPR, eller Dataskyddsförordningen som den också kallas, innehåller regler om hur man får behandla personuppgifter. Förordningen gäller från 25 maj 2018 och har ersatt personuppgiftslagen (PuL).

KÄNSLIGA PERSONUPPGIFTER

Det begrepp som användes tidigare i personuppgiftslagen. Dessa har nu ersatts av benämningen särskilda kategorier av personuppgifter.

PERSONUPPGIFTER

All slags information som antingen direkt eller indirekt kan identifiera en nu levande person – såsom namn, IP-adress, fotografier, löneuppgifter. De individer som företaget behandlar personuppgifter om kallas registrerade, dvs de personer som det finns information om.

Personuppgiftsbehandling. Varje åtgärd som, helt eller delvis automatiserat, vidtas med personuppgifter. Behandling innefattar:

- Inhämtning; insamling, framtagning, registrering.
- Hantering; bearbetning, ändring, läsning, användning, justering, sammanförande, strukturering, organisering och begränsning.
- Delning; överföring, spridning, tillhandahållande.
- Gallring; lagring, radering, förstöring.

PERSONUPPGIFTSANSVARIG

Normalt juridisk person eller myndighet som bestämmer vilka uppgifter som behandlas till vad och vad de ska användas till. All behandling som en anställd gör i sitt arbete är arbetsgivaren personuppgiftsansvarig för.

PERSONUPPGIFTSBITRÄDE

Företag eller person som hanterar personuppgifter åt annan personuppgiftsansvarig.

Ett företag eller organisation som behandlar personuppgifter på uppdrag av den personuppgiftsansvarige och för dennes räkning, exempelvis en tjänsteleverantör som inom ramen för sin leverans får tillgång till personuppgifter. Det kan vara en IT-leverantör eller ett anlitat bolag med uppdrag att sköta löneprocessen.

PERSONUPPGIFTSBITRÄDESAVTAL
Avtal kring personuppgiftsbiträdets rätt att behandla personuppgifter i enlighet med instruktionerna från den personuppgiftsansvarige.

PERSONUPPGIFTSLAGEN (PUL)
Svensk lagstiftning från 1995 för personuppgiftsbehandling. Upphörde när GDPR trädde i kraft 25 maj 2018.

PRIVACY BY DEFAULT
IT-system ska vara designade så standardfallet är att den som behandlar personuppgifter inte behandlar personuppgifter i onödan.

PRIVACY BY DESIGN
IT-system ska vara designade med inbyggt skydd av den personliga integriteten så att man tar hänsyn till integritetsskyddsreglerna redan när man utformar IT-system och rutiner.

PRIVACY SHIELD
Överenskommelse om skydd för personuppgifter mellan EU och USA.

REGISTRERADE
Alla individer som personuppgifterna berör. Dessa registrerade kan finnas inom en organisation, såsom anställda, i medlemsorganisationer som medlem, men även personer utanför en organisation som kunder och kunders anställda.

SALK
SALK, Svensk standard för Auktoriserade Lönekonsulter, är en unik produkt framtagen av Srf konsulterna för lönebranschen och kan ses som en bruksanvisning för löneprocesser. Den är också normgivande för Auktoriserade Lönekonsulter. I SALK ingår definitioner och beskrivningar av delmoment och mål samt identifiering av löneprocesser där standarden är tillämplig.

SAMTYCKE
Tillåtelse av den registrerade att behandla personuppgifter utifrån tydligt syfte. Samtycke ska vara frivilligt och kunna återkallas. Den registrerade måste ha fått information om personuppgiftsbehandlingen. Samtycke är som rättslig grund en begränsad möjlighet i relationen arbetsgivare - arbetstagare.

SRF LÖNSAM
Srf Lönsam är en samverkan mellan Srf konsulterna och Sveriges ledande lönesystemleverantörer; Aditro Enterprise AB, Agrando AB, Bluegarden AB, Caspeco AB, DataVara AB, Fortnox AB, Flex Applications AB, Hogia Professional Services AB, HRM Software AB, Kontek Lön AB, Nmbrs Sweden AB, SoftOne Sverige AB, Swelön AB, Unit4 AB, SAP Svenska AB, Visma Enterprise AB, Visma Spcs AB.

SÄRSKILDA KATEGORIER AV PERSONUPPGIFTER
Personuppgifter som enligt GDPR artikel 9 kräver särskilda skäl för att få hanteras; 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.