

DEN 22 APRIL 2025

LATHUND GDPR

HASTIGHETSEFTERLEVNAD

LATHUND: Integritetsarbetet – steg för steg

En vägledning för att säkerställa att personuppgiftsbehandlingen sker i enlighet med GDPR och med hänsyn till de anställdas integritet. Detta är en komprimerad version av Integritetsstegen nedan.

STEG 1: Klargör och dokumentera behov och ändamål

- Identifiera, klargör och formulera behovet av behandlingen.
- Beskriv tydligt och konkret ändamålen med behandlingen.
- Dokumentera behoven, ändamålen och ställningstaganden.

STEG 2: Gör en konsekvensbedömning

- Beskriv systematiskt den planerade behandlingen, dess syften och berättigade intresse.
- Bedöm behovet och proportionaliteten av behandlingen i förhållande till syftet.
- Identifiera och bedöm riskerna för de anställdas rättigheter och friheter.
- Redogör för åtgärder för att hantera riskerna (skyddsåtgärder, säkerhetsåtgärder och rutiner).
- Involvera anställda och deras företrädare tidigt i processen.

STEG 3: Begär förhandssamråd med IMY

Om konsekvensbedömningen visar på fortsatt hög risk för den enskildes fri- och rättigheter:

- Skicka en begäran till IMY innan behandlingen påbörjas.
- Använd IMY:s blankett: [IMY:s webbsida](#).
- Beskriv behandlingens syfte, tekniska och organisatoriska åtgärder samt kvarstående risker.

STEG 4: Ansök om tillstånd

Om behandlingen innefattar lagöverträdelser:

- Ansök om tillstånd från IMY.
- Beskriv behandlingen och hur den följer GDPR:s grundprinciper.
- Redovisa vem som behandlar uppgifterna och om det finns delat personuppgiftsansvar.
- Redogör för rättsliga grunder och åtgärder för att skydda personuppgifter.

STEG 5: Fastställ den rättsliga grunden

- Motivera varför behandlingen är nödvändig för ett berättigat intresse.
- Bedöm om anställdas fri- och rättigheter väger tyngre än det berättigade intresset.
- Redogör för tekniska och organisatoriska skyddsåtgärder.

STEG 6: Säkerställ efterlevnad av GDPR

- Se till att behandlingen är laglig, korrekt och transparent.
- Begränsa behandlingen till det nödvändiga (dataminimering).
- Upprätthåll noggrannhet, lagringsbegränsning och säkerhet.
- Dokumentera alla åtgärder och uppdatera vid behov.

Om Integritetsstegen

Integritetsstegen är framtagna inom ramen för projektet Hållbara hastigheter. Den riktar sig främst till entreprenörer, i sin egenskap av arbetsgivare och personuppgiftsansvarig, som ska uppfylla upphandlingskravet avseende hastighetsredovisning (nedan Kravet) i sin avtalsrelation med beställaren (Trafikverket). Integritetsstegen är tänkt att fungera som ett informationsstöd och en introduktion i arbetet med att beakta frågor om de anställdas integritet utifrån den dataskyddsrättsliga regleringen vid genomförandet av Kravet och är avgränsad till situationer då arbetsgivaren inte är en myndighet.

Integritetsstegen tar sikte på personuppgiftsbehandling med *intresseavvägning* som rättslig grund (se ordlistan i del 2) eftersom det är den grund som kan aktualiseras för icke-myndigheter i en arbetsrättslig avtalsrelation. Integritetsskyddsmyndigheten (IMY) har också prövat denna rättsliga grund i en tillståndsprövning avseende personuppgifter som rör lagöverträdelse gällande hastighetsmätning. I det specifika beslutet beviljades tillstånd, men det ska betonas att tillståndsprövningen är individuell och beror på omständigheterna i det enskilda fallet. Varje entreprenör ska därför göra sin egen integritetsanalys och i en tillståndsansökan visa att den planerade personuppgiftsbehandlingen har stöd i en rättslig grund. Vidare ska den som är personuppgiftsansvarig visa att personuppgifterna kommer att hanteras i enlighet med de dataskyddsrättsliga och arbetsrättsliga kraven.

Integritetsstegen kan ses som en översiktlig och introducerande metod för att belysa integritetsarbetet steg för steg utifrån olika dataskyddsrättsliga teman och frågeställningar som aktualiseras. Syftet är att ge information om de dataskyddsrättsliga krav som behöver hanteras vid personuppgiftsbehandling i den ovan nämnda situationen. **Integritetsstegen ska inte betraktas som en uttömmande checklista av alla dataskyddskrav som kan aktualiseras i det specifika fallet.** Den som är personuppgiftsansvarig entreprenör behöver själv göra en analys och beakta omständigheterna i det enskilda specifika fallet och hur de förhåller sig till de rättsliga kraven. Förhoppningsvis kan Integritetsstegen fungera som ett översiktligt informationsstöd eller introduktion i detta arbete.

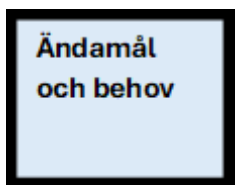
Integritetsstegen är indelad i två delar. I del 1 beskrivs det dataskyddsrättsliga integritetsarbetet steg för steg utifrån sex teman: (1) ändamål och behov, (2) konsekvensbedömning, (3) förhandssamråd, (4) ansökan om tillstånd, (5) rättslig grund, samt (6) grundläggande principer. Det ska nämnas att det dataskyddsrättsliga temat och begreppet rättslig grund (steg 5) liksom grundläggande dataskyddsrättsliga principer (steg 6) behöver hanteras inom ramen för en konsekvensbedömning (steg 2), förhandssamråd (steg 3) respektive en ansökan om tillstånd (steg 4). Att de behandlas i efterföljande steg 5 och 6 motiveras av en mer utförlig redogörelse för vad som krävs avseende rättslig grund och dataskyddsrättsliga grundläggande principer i förhållande till en tillståndsansökan (steg 4). Del I avslutas med en kort hänvisning till och exemplifiering av arbetsrättsliga krav rörande integritetsaspekter och integritetsarbete.

I del 2 följer en lista på annan relevant läsning som kan vara av intresse i integritetsarbetet. I del 2 återfinns också en ordlista som förklarar de dataskyddsrättsliga begrepp som förekommer i Integritetsstegen.

DEL 1

Integritetsarbetet – steg för steg

STEG 1 Klargör behov och ändamål

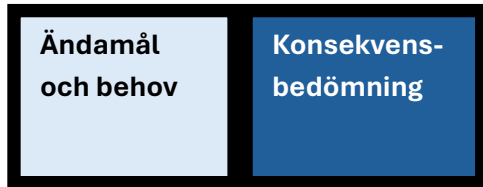


Artikel 5 GDPR

Det första steget innebär ett arbete med att klargöra och fastställa vilket eller vilka syften som finns med den personuppgiftsbehandling som planeras. Frågorna som behöver ställas är vad det finns för behov av och anledning till att behandla personuppgifter för hastighetsmätning. Detta steg är centralt i integritetsanalysen eftersom de dataskyddsrättsliga kraven kommer att bedömas mot det fastställda ändamålet och behovet. Bland annat får uppgifterna enbart samlas in för de särskilda, uttryckligt angivna och berättigade ändamål som fastställts. Uppgifterna får inte heller senare behandlas på ett sätt som inte stämmer överens med dessa ändamål. Det är därför viktigt att man beskriver och klargör behov och ändamål på ett tydligt och väl genomtänkt sätt. Varje behandling ska ha ett tydligt ändamål som ska vara fastställt när personuppgifter samlas in. För att det ska vara ett berättigat ändamål måste det också vara kopplat till en rättslig grund (se steg 5).

- Identifiera, klargör och formulera behovet/behoven av behandlingen
- Beskriv tydligt, specifikt och konkret för vilka ändamål behandling ska ske
- Dokumentera de fastställda behoven, ändamålen och era ställningstaganden

STEG 2 Gör en konsekvensbedömning



Artikel 35.1 GDPR

Typen av ändamål påverkar vilka risker som finns eller uppstår med personuppgiftsbehandlingen. Behandling som syftar till att kartlägga eller övervaka arbetstagare innebär till exempel stora integritetsrisker, liksom behandling som syftar till att vidta åtgärder som får negativa konsekvenser för arbetstagaren. Det är därför viktigt att identifiera och lyfta fram sådana risker så att de kan konsekvensbedömas.

Integritetsstegens andra steg innebär ett framtagande av en konsekvensbedömning avseende dataskydd. En sådan bedömning ska göras om personuppgiftsbehandlingen "sannolikt leder till en hög risk för fysiska personers rättigheter och friheter". Risker ska i första hand bedömas utifrån dataskydd och integritet. Eftersom anställda betraktas som sårbara personer ska en konsekvensbedömning alltid genomföras inom ramen för ett anställningsförhållande. Personuppgiftsbehandling som rör lagöverträdelser är också att betrakta som en hög risk för fysiska personers rättigheter och friheter.

Konsekvensutredningen bör påbörjas i ett så tidigt skede som möjligt, även om inte alla delar av en behandling är kända. Konsekvensbedömningen ska regelbundet följas upp och omvärderas vid behov eftersom ändrade förhållanden och riskbedömningen kan kräva det. Det bör därför betonas att en konsekvensbedömning inte är en engångsaktivitet utan ett regelbundet och kontinuerligt arbete med att identifiera, analysera, uppskatta, utvärdera och avhjälpa risker med personuppgiftsbehandling.

Konsekvensbedömningen ska innehålla i vart fall följande:

- a) *en systematisk beskrivning av den planerade behandlingen och behandlingens syften samt i de fall det är aktuellt, den personuppgiftsansvariges berättigade intresse,*

Det här betyder att behandlingens art, omfattning, sammanhang och ändamål ska finnas med. En funktionell beskrivning av behandlingen ska också finnas. Beskrivningen ska redogöra för registreringen av personuppgifter, mottagare och den period man avser lagra uppgifterna. Dessutom ska tillgångar, såsom till exempel maskin- och programvara

och nätverk vara identifierade och framgå. Efterlevnad av tillämpliga godkända uppförandekoder ska också beaktas.

b) en bedömning av behovet av och proportionaliteten hos behandlingen i förhållande till syftena,

Enligt denna punkt ska de planerade åtgärderna som fastställts för att visa att GDPR efterlevs framgå. Detta innebär att de åtgärder som bidrar till att behandlingen är proportionell och nödvändig i förhållande till särskilda, uttryckligt angivna och berättigade ändamål ska finnas med. Det ska framgå att och på vilket sätt:

- behandlingen har en rättslig grund (se mer i steg 5),
- uppgifterna är adekvata, relevanta och inte för omfattande (se också steg 6),
- lagringstiden är begränsad (se också steg 6)

Åtgärder som stärker arbetstagarnas rättigheter ska också framgå i konsekvensbedömningen. Det ska bland annat redogöras för:

- vilken information om behandlingen som tillhandahålls de anställda,
- förhandssamråd (se steg 3),
- rätt till rättelse och radering, rätt att göra invändning, rätt till begränsning av behandling,
- förhållandet till eventuella personuppgiftsbiträden.

c) en bedömning av risker för de anställdas rättigheter och friheter,

I denna del ska en uppskattning av riskens ursprung, art, särdrag och allvar göras. Varje risk, såsom till exempel risken för obehörig åtkomst, oönskad ändring och att uppgifter försvinner, ska beaktas ur de anställdas perspektiv. Möjliga konsekvenser för de anställdas rättigheter och friheter vid sådana händelser ska identifieras. Även hot som kan leda till obehörig åtkomst, oönskad ändring och förlust av uppgifter ska identifieras. En uppskattning ska göras av sannolikhetsgrad och allvar.

d) åtgärder som planeras för att hantera riskerna. Detta innefattar skyddsåtgärder, säkerhetsåtgärder och rutiner för att säkerställa skyddet av de anställdas personuppgifter och för att visa att GDPR efterlevs.

Åtgärderna som ska användas för att hantera de identifierade riskerna ska redogöras för. De kan vara av organisatorisk eller teknisk karaktär.

I arbetet med konsekvensbedömningen kan det vara lämpligt att involvera de anställda och förhöra sig om vilka möjliga risker och konsekvenser de ser med personuppgiftsbehandlingen. Det ska dokumenteras om den personuppgiftsansvariga entreprenören och de anställda inte har samma uppfattning rörande personuppgiftsbehandlingen. Det ska också dokumenteras om entreprenören väljer att inte tillfråga de anställda om detta. Detsamma gäller de anställdas företrädare, såsom

förekommande arbetstagarorganisationer. Dessa företrädare bör därför involveras i ett tidigt skede för dialog kring frågor avseende den aktuella personuppgiftsbehandlingen, risker för de anställda och integritetshänsyn.

- Beskriv på ett systematiskt sätt den planerade behandlingen, dess syften och den personuppgiftsansvariges berättigade intresse av behandlingen
- Bedöm behovet och proportionaliteten av behandlingen i förhållande till syftet
- Identifiera och bedöm riskerna för de anställdas rättigheter och friheter
- Beskriv de åtgärder som planeras för att hantera de identifierade riskerna

STEG 3 Begär förhandssamråd med IMY



Artikel 36 GDPR

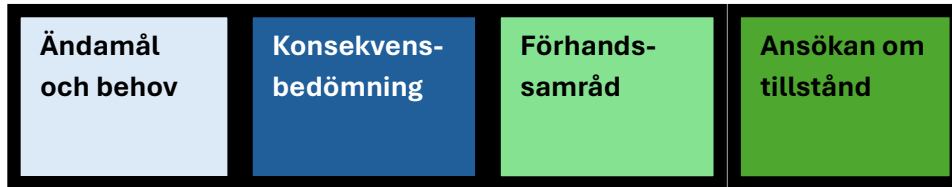
I det fall konsekvensbedömningen är utförd och bedömningen är att det fortfarande finns en hög risk för enskildas fri- och rättigheter ska en begäran om förhandssamråd med IMY göras innan behandlingen påbörjas. IMY har tagit fram en särskild blankett för en sådan begäran som finns tillgänglig på IMY:s webbsida, se

<https://www.imy.se/globalassets/dokument/blanketter/blankett-forhandssamrad.pdf>.

Den kan fyllas i och skickas digitalt till IMY. Förutom uppgifter om personuppgiftsansvarig eller personuppgiftsbiträde samt kontaktperson ska syftet med personuppgiftsbehandlingen beskrivas kortfattat i blanketten. Därutöver ska tekniska och organisatoriska åtgärder, säkerhetsåtgärder och garantier beskrivas. Även de kvarstående höga riskerna efter vidtagna åtgärder ska redovisas. Det ska också redovisas varför de kvarstående riskerna inte kunnat åtgärdas fullt ut, till exempel utifrån att de inte kan begränsas tillräckligt genom rimliga åtgärder med avseende på teknik och kostnader. Under förutsättning att den personuppgiftsansvarige entreprenören har gjort en gedigen konsekvensbedömning kan de nämnda uppgifterna hämtas direkt från denna. Dessutom ska konsekvensbedömningen bifogas begäran om samråd.

I det fall det har konstaterats att personuppgiftsbehandlingen avser lagöverträdelser krävs enskilt tillstånd från IMY. Den personuppgiftsansvarige entreprenören kan då, enligt IMY, välja att ansöka direkt om sådant tillstånd från IMY utan föregående samråd. Stäm därför av med IMY i det specifika fallet.

STEG 4 Ansök om tillstånd



6 § förordningen (2018:219) med kompletterande bestämmelser till EU:s dataskyddsförordning

Mot bakgrund av att entreprenören behandlar personuppgifter i samband med hastighetsmätning aktualiseras frågan om tillåtligheten att behandla uppgifter om lagöverträdelse. Som utgångspunkt får inte andra än myndigheter behandla sådana uppgifter, men IMY får i enskilda fall besluta om undantag genom en tillståndsprövning. Entreprenören kan, i sin egenskap av personuppgiftsansvarig, därför välja att ansöka om ett sådant tillstånd från IMY.

Följande information ska enligt IMY framgå av ansökan:

- en beskrivning av den behandling som planeras och hur den följer de grundläggande principerna i GDPR (se mer i steg 1,2 och 6),
- uppgift om vem eller vilka som ska behandla personuppgifterna och om det finns ett delat personuppgiftsansvar,
- uppgift om ändamålen med behandlingen (se steg 1),
- de rättsliga grunderna för de behandlingar som planeras för de olika ändamålen (se mer i steg 5),
- en förklaring till varför den eller de åberopade rättsliga grunderna är tillämpliga (se mer i steg 5).

När det gäller beskrivningen av behandlingen avseende hastighetsmätning är det viktigt med en ingående redogörelse för den teknik som ska användas och hur hastighetsmätningen går till. Vidare ska beskrivas hur data analyseras och presenteras. Beskrivningen av behandlingen är grundläggande för att kunna bedöma dess överensstämmelse med GDPR och kraven på rättslig grund (se steg 5) och de grundläggande dataskyddsrättsliga principerna (se steg 6). Det är också av vikt att beskriva de organisatoriska skyddsåtgärder man vidtagit eller avser vidta avseende behandlingen, såsom till exempel informations- och utbildningsåtgärder. Har entreprenören gjort en grundlig konsekvensutredning kan en stor del av innehållet i ansökan hämtas därifrån.

STEG 5 Fastställ den rättsliga grunden



Artikel 6 GDPR

Vid en ansökan om tillstånd för personuppgiftsbehandling som rör lagöverträdelser inom ramen för hastighetsmätning måste den rättsliga grunden för sådan behandling anges. Den rättsliga grund som kan bli aktuell i anställningsförhållandet mellan den personuppgiftsansvarige entreprenören och dennes anställda är *intresseavvägning*.

Med intresseavvägning som rättslig grund får personuppgifter lämnas ut till tredje man, det vill säga någon annan (såsom beställaren). Detta under förutsättning att tredje man har ett berättigat intresse. Innan uppgifterna lämnas ut ska den personuppgiftsansvarige ta reda på varför tredje man vill ha personuppgifterna, om de verkligen behöver uppgifterna och vad de ska användas till. Den personuppgiftsansvarige måste också kunna visa att utlämnandet av uppgifterna är motiverat. Däremot är det tredje man som är ansvarig för att i sin tur fastställa vilken rättslig grund de stödjer sin egen behandling på.

För att entreprenören ska kunna stödja sig på intresseavvägning som rättslig grund krävs att entreprenören kan visa att:

- 1) det finns ett berättigat intresse för behandlingen,
- 2) behandlingen av personuppgifter är nödvändig för ett ändamål som rör det berättigade intresset och
- 3) att de anställdas grundläggande fri- och rättigheter inte väger tyngre än det berättigade intresset.

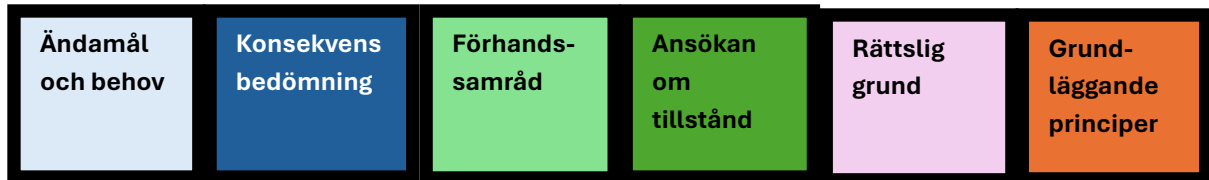
När det gäller kravet på ett berättigat intresse är det viktigt att tydligt klargöra ändamålen med personuppgiftsbehandlingen eftersom ändamålen sätter ramarna för vad man får göra enligt GDPR. I bedömningen av om intresset är berättigat beaktas om intresset är ett faktiskt intresse. Det får inte vara fråga om intressen som är alltför vaga eller spekulativa eftersom sådana inte tillräckligt motiverar behandling. En annan aspekt som beaktas är om den personuppgiftsansvarige entreprenören agerar inte bara i sitt eget intresse utan också i hela samhällets intresse. Då väger intresset i regel tyngre. För att

motivera hastighetsmätning har till exempel ändamål som arbetsmiljöska, trafiksäkerhetsska och miljöska förekommit i IMY:s olika beslut om tillstånd och förhandssamråd. Att öka trafiksäkerheten och minska risken för olyckor har bedömts som ett berättigat intresse. Det är dock viktigt att poängtera att undantag för personuppgiftsbehandling som rör lagöverträdelser prövas i det enskilda fallet. Undantaget prövas då utifrån kraven på rättslig grund, grundläggande dataskyddsrättsliga principer och de organisatoriska och tekniska skyddsåtgärder som den enskilde entreprenören vidtagit.

När intresset har angetts och motiverats som berättigat behöver entreprenören också visa att behandlingen är nödvändig för det berättigade intresset. Personuppgifter får inte behandlas om syftet med behandlingen kan uppnås genom andra, mindre integritetskränkande, medel. Entreprenören behöver därför beakta om det finns alternativa sätt att uppnå det angivna syftet med behandlingen. I en ansökan om tillstånd behöver entreprenören motivera varför behandlingen är nödvändig med beaktande av eventuella alternativa medel. Entreprenören behöver också visa på att syftet med behandlingen inte rimligen kan uppnås på ett lika effektivt sätt genom dessa alternativa åtgärder.

När entreprenören motiverat varför intresset av behandlingen är berättigat och att behandlingen är nödvändig för att uppnå syftet, ska entreprenören visa att de anställdas grundläggande fri- och rättigheter inte väger tyngre än det berättigade intresset. För att kunna visa detta behöver man beakta vilka konsekvenser behandlingen kan få för de anställda mot bakgrund av de tekniska och organisatoriska skyddsåtgärder entreprenören vidtagit eller kommer att vidta. Det är därför viktigt att entreprenören i ansökan redogör ingående för dessa åtgärder. Det kan till exempel handla om avidentifieringsmetoder, aggregering av data, ökad insyn, ett inbyggt integritetsskydd, utbildning och informationsåtgärder. Vid IMY:s prövning beaktas också typen av personuppgiftsbehandling och hur denna konkret går till. IMY beaktar aspekter som hur många personer som kommer att ha tillgång till personuppgifterna, formerna för deras åtkomst, samt risken för att allmänheten kan få tillgång till personuppgifterna. I bedömningen tas också i beaktande om de anställda rimligen kan förvänta sig, till exempel mot bakgrund av sin utbildning och sina anställningsavtal, att deras personuppgifter kan komma att behandlas utifrån syftet med behandlingen. Entreprenören bör därför redogöra för sin inställning avseende de anställdas förväntningar i förhållande till behandlingen.

STEG 6 Säkerställ överensstämmelse med grundläggande dataskyddsrättsliga principer



Artikel 5 GDPR

Utöver en motivering av den rättsliga grund som entreprenören stödjer sig på ska entreprenören också visa att den planerade personuppgiftsbehandlingen överensstämmer med de grundläggande dataskyddsrättsliga principerna. Principerna utgör kärnan i GDPR och gäller för all personuppgiftsbehandling. De sätter de yttersta ramarna för vad som är en tillåten behandling. Att principerna beaktas vid behandlingen prövas vid en ansökan om tillstånd. Den personuppgiftsansvarige ska då kunna visa att behandlingen är förenlig med dessa. Därför behöver entreprenören beskriva hur personuppgiftsbehandlingen förhåller sig till följande grundläggande dataskyddsrättsliga principer:

- a) principen om laglighet, korrekthet och öppenhet som innebär att uppgifterna ska behandlas på ett lagligt, korrekt och öppet sätt i förhållande till den registrerade;
- b) principen om ändamålsbegränsning som innebär att uppgifterna ska samlas in för särskilda, uttryckligt angivna och berättigade ändamål och inte senare behandlas på ett sätt som är oförenligt med dessa ändamål;
- c) principen om uppgiftsminimering som går ut på att uppgifterna ska vara adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka de behandlas;
- d) principen om riktighet som betyder att uppgifterna ska vara riktiga och om nödvändigt uppdaterade. Dessutom ska alla rimliga åtgärder vidtas för att säkerställa att personuppgifter som är felaktiga i förhållande till de ändamål för vilka de behandlas raderas eller rättas utan dröjsmål;
- e) principen om lagringsminimering innebär att uppgifterna inte får förvaras i en form som möjliggör identifiering av den registrerade under en längre tid än vad som är nödvändigt för de ändamål för vilka personuppgifterna behandlas; samt
- f) principen om integritet och konfidentialitet som betyder att uppgifterna ska behandlas på ett sätt som säkerställer lämplig säkerhet för personuppgifterna, inbegripet skydd

mot obehörig eller otillåten behandling, med användning av lämpliga tekniska eller organisatoriska åtgärder.

Den personuppgiftsansvarige behöver, utifrån det ovan redovisade, säkerställa och i ansökan redogöra för att (och hur):

- personuppgiftsbehandlingen har stöd i GDPR,
- personuppgifterna endast kommer att samlas in för specifika, särskilt angivna och berättigade ändamål,
- de personuppgifter som ska behandlas inte är fler än vad som är nödvändigt för att ändamålen ska uppnås,
- personuppgifterna är riktiga,
- personuppgifterna kommer att raderas när de inte längre behövs,
- personuppgifterna kommer att skyddas genom tekniska och organisatoriska åtgärder (beskriv dessa utförligt), samt
- GDPR i övrigt efterlevs.

Kort om integritetsarbetet och arbetsrättsliga krav

Integritetsstegen och dess sex steg som beskrivits ovan har tagit sikte på att ge en dataskyddsrättslig introduktion i arbetet med att ta sig an och genomföra Kravet. Som nämnts är Integritetsstegen avgränsad till situationer då den personuppgiftsansvarige arbetsgivaren inte är en myndighet och avseende personuppgiftsbehandling utifrån den rättsliga grunden intresseavvägning.

Utöver iakttagande av dataskyddsrättsliga krav behöver det betonas att entreprenören, i sin egenskap av arbetsgivare, också har att iaktta relevanta tillämpliga arbetsrättsliga krav. Dessa krav och arbetsrättens syn på integritetsaspekter och integritetsskydd behandlas inte närmare i Integritetsstegen, men i exemplifierande syfte kan pekas på vikten av att:

- involvera arbetstagarna i integritetsarbetet
- informera arbetstagarna om personuppgiftsbehandlingen
- se över och initiera ev. utbildningsinsatser
- involvera och informera fackliga organisationer
- beakta ev. förhandlingsskyldighet
- beakta lag och god sed på arbetsmarknaden

DEL 2

Vidare läsning

Böcker

- GDPR-guiden - Handbok för verkligheten
Öhman, Hanna och Värmon, Didrik. (2022). Norstedts juridik.
- Dataskyddsförordningen (GDPR) m.m. : en kommentar
Öman, Sören. (2024) Norstedts juridik.
- GDPR - Förstå och tillämpa i praktiken
Wendleby, Monika och Wetterberg, Dag. (2018). Sanoma utbildning.
- Dataskyddsförordningen GDPR - Hantera registrerades rättigheter.
Wendleby, Monika. (2021). Sanoma utbildning.
- GDPR för dataskyddsombud och andra ansvariga.
Wendleby, Monika. (2020). Sanoma utbildning.
- Anställdas integritetsskydd – och dataskyddsförordningen
Grahn, Erik och Kjällström, Susanna. (2017). Wolters Kluwer.

Beslut och förhandssamråd

- Beslut om tillstånd att behandla personuppgifter om lagöverträdelser, diarienummer DI-2022-253 (IMY, 2023).
- Beslut efter tillsyn enligt dataskyddsförordningen, diarienummer IMY-2022-6656 (IMY, 2023).
- Förhandssamråd om behandling av personuppgifter vid användning av elektroniska körjournaler med ISA-funktion, diarienummer DI-2021-1227 (IMY, 2021).
- Förhandssamråd om behandling av personuppgifter vid användning av elektroniska körjournaler med ISA-funktion, diarienummer DI-2021-703 (IMY, 2021).

Övrigt

- Integritetsskyddsmyndighetens webbsida: <https://www.imy.se/>
- EDPB:s GDPR-guide för små och medelstora företag
https://www.edpb.europa.eu/sme-data-protection-guide/home_sv.
- Rättsligt ställningstagande IMYRS 2021:1 – innebörden av begreppet ”personuppgifter som rör lagöverträdelser som innefattar brott” i artikel 10 i dataskyddsförordningen. (IMY, 2021)

Ordlista

Begränsning av behandling

En rättighet som innebär att man har rätt till begränsning av behandling. Begränsningen innebär att uppgifterna bara får behandlas för vissa syften. Denna rättighet kan användas i väntan på att felaktiga uppgifter rättas eller under tiden en personuppgiftsansvarig utreder om en uppgift kan raderas.

Behandling

Se nedan om Personuppgiftsbehandling.

Berättigat intresse

Berättigat intresse är en rättslig grund för behandling. För att kunna använda sig av rättslig grund måste man först göra en intresseavvägning.

Berättigat ändamål

En behandling måste ha ett ändamål. Till ändamålet ska det finnas en rättslig grund kopplat. Annars är ändamålet inte berättigat. Exempelvis kan en arbetsgivares ändamål vara att rapportera skatteuppgifter gällande sina anställda. Den rättsliga grunden är då rättslig förpliktelse och ändamålet anses berättigat.

Dataskyddsförordningen

Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning). Förkortas GDPR.

Dataskyddslagen

Lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning.

Grundläggande dataskyddsrättsliga principer

Grundläggande principer som följer av GDPR och innebär att den personuppgiftsansvariga

- måste ha stöd i GDPR för att få behandla personuppgifter,
- endast får samla in personuppgifter för specifika, särskilt angivna och berättigade ändamål,
- inte ska behandla fler personuppgifter än vad som är nödvändigt för att ändamålen ska uppnås,

- ska se till att personuppgifterna är riktiga,
- ska radera personuppgifterna när de inte längre behövs,
- ska skydda personuppgifterna genom tekniska och organisatoriska åtgärder, samt
- kunna visa att GDPR följs och på vilket sätt.

Den registrerade

En fysisk person som kan identifieras genom en personuppgift eller genom att flera personuppgifter läggs samman.

Förhandssamråd

I det fall konsekvensbedömningen är utförd och bedömningen är att det fortfarande finns en hög risk för enskildas fri- och rättigheter ska ett förhandssamråd med IMY göras innan behandlingen påbörjas.

Integritetsanalys

Integritetsanalys innebär en analys av om en behandling av personuppgifter är förenlig med bestämmelser om skyddet för den personliga integriteten. En del av analysen innebär att konsekvenserna för den personliga integriteten vägs mot om de är nödvändiga och proportionerliga mot det man vill uppnå med behandlingen.

Integritetsarbete

Integritetsarbete innebär en personuppgiftsansvarigs arbete med att skydda och respektera personlig integritet, bland annat genom att följa GDPR och annan dataskyddsreglering.

Intresseavvägning

Intresseavvägning innebär att man måste säkerställa att intresset att behandla en personuppgift väger tyngre än den registrerades intresse.

Invändning mot behandling

En rättighet som innebär att man har rätt att invända mot behandling. Den personuppgiftsansvariga är skyldig att informera om denna rättighet vid första kontakttillfället.

Konsekvensbedömning

En konsekvensbedömning ska göras om personuppgiftsbehandlingen "sannolikt leder till en hög risk för fysiska personers rättigheter och friheter". Syftet är att förebygga risker och skydda människors fri- och rättigheter.

Nödvändig behandling

I flera rättsliga grunder finns begreppet nödvändig. Begreppet nödvändig har inte samma betydelse som i dagligt tal. Även om en uppgift kan utföras utan att personuppgifter behandlas kan behandlingen ändå anses vara nödvändig om behandlingen leder till effektivitetsvinster.

Personuppgift

En uppgift som ensam eller tillsammans med fler uppgifter kan identifiera en levande fysisk person.

Personuppgiftsbiträde

Personuppgiftsbiträdet behandlar personuppgifter för den personuppgiftsansvarigas räkning. Personuppgiftsbiträdet finns alltid utanför den personuppgiftsansvarigas organisation och kan exempelvis vara ett företag som anlitas för att ta hand om utskick och marknadsföring eller ett molntjänstföretag som anlitas för att lagra uppgifter.

Personuppgiftsansvarig

Personuppgiftsansvarig är en fysisk eller juridisk person som bestämmer för vilka ändamål uppgifter ska behandlas och hur denna behandling ska gå till. Rättsliga förpliktelser följer av lag eller annan författning, av kollektivavtal eller genom beslut som meddelats med stöd av lag (till exempel myndighetsbeslut).

Personuppgiftsbehandling

Behandling är ett samlat begrepp för olika sorter hanteringar av personuppgifter. I dataskyddsförordning anges att exempelvis insamling, registrering, organisering, lagring och radering är olika typer av behandling.

Principen om integritet och konfidentialitet

En av de grundläggande dataskyddsrättsliga principerna. Principen betyder att personuppgifterna ska behandlas på ett sätt som säkerställer lämplig säkerhet för personuppgifterna.

Principen om laglighet, korrekthet och öppenhet

En av de grundläggande dataskyddsrättsliga principerna. Principen innebär att personuppgifterna ska behandlas på ett lagligt, korrekt och öppet sätt i förhållande till den registrerade.

Principen om lagringsminimering

En av de grundläggande dataskyddsrättsliga principerna. Principen innebär att personuppgifterna inte får förvaras i en form som möjliggör identifiering av den

registrerade under en längre tid än vad som är nödvändigt för de ändamål för vilka personuppgifterna behandlas.

Principen om riktighet

En av de grundläggande dataskyddsrättsliga principerna. Principen innebär att personuppgifterna ska vara riktiga och uppdaterade.

Principen om uppgiftsminimering

En av de grundläggande dataskyddsrättsliga principerna. Principen innebär att personuppgifterna ska vara adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka de behandlas.

Principen om ändamålsbegränsning

En av de grundläggande dataskyddsrättsliga principerna. Principen innebär att uppgifterna ska samlas in för särskilda, uttryckligt angivna och berättigade ändamål och inte senare behandlas på ett sätt som är oförenligt med dessa ändamål.

Radering av behandling

En rättighet som innebär att man i de flesta fall har rätt till radering av personuppgifter om man begär detta. Den personuppgiftsansvariga kan bland annat neka radering om behandlingen krävs för att uppfylla en rättslig förpliktelse.

Riskbedömning

I riskbedömningen görs en bedömning av om behandlingen av personuppgifter leder till en sannolik hög risk för enskilda personers fri- och rättigheter. I Riskbedömningen analyseras vilka risker som finns och vilka säkerhetsåtgärder som kan krävas. Utifrån riskbedömningen fattas beslut om man ska göra en konsekvensbedömning.

Rättelse av behandling

En rättighet som innebär att man har rätt att begära att felaktiga personuppgifter rättas.

Rättslig grund

Enligt GDPR ska minst en rättslig grund föreligga. I GDPR finns följande rättsliga grunder.

- Samtycke från den registrerade
- Avtal med den registrerade
- Nödvändig på grund av en rättslig förpliktelse
- Nödvändig på grund av allmänt intresse

- Led i myndighetsutövning
- Intresseavvägning
- Skydd av grundläggande intresse när den registrerade inte kan ge samtycke.

Ändamål för behandling

Behandlingar ska ha ett tydligt definierat ändamål. Den personuppgiftsansvarige ska när personuppgifter samlas in redan ha klargjort de ändamål som uppgifterna samlas in för.