



Positioneringsteknik i arbetslivet

Det har blivit allt vanligare att arbetsgivare använder olika former av positioneringssystem för att kontrollera var fordon och anställda befinner sig. När sådana system används behandlas i de flesta fall personuppgifter som regleras av personuppgiftslagen (* se not på nästa sida).

Positioneringssystem möjliggör en närgående övervakning av enskilda individer och medför risker för otillbörliga integritetsintrång. Personuppgiftslagens regler till skydd för den personliga integriteten fyller här en viktig funktion. Den här checklistan visar vilka krav personuppgiftslagen ställer.

Utgå från att personuppgiftslagen gäller

- Även om positioneringssystem sällan innehåller uppgifter som direkt går att knyta till enskilda individer – till exempel personnamn – går det ofta med tjänstgöringslistor eller på annat sätt att knyta fordonen i systemen till enskilda individer. En sådan indirekt koppling är tillräcklig för att personuppgiftslagen ska gälla.
- Det finns EU-regler för kör- och vilotider samt regler om färdskrivare vid vägtransporter. Datainspektionen ser inte något principiellt hinder enligt personuppgiftslagen mot att arbetsgivare använder positioneringsteknik för att uppfylla de krav som dessa regelverk ställer.

Klargör personuppgiftsansvaret

Personuppgiftsansvarig är normalt den juridiska person som behandlar personuppgifter i sin verksamhet (ett företag, en myndighet eller en organisation) och som bestämmer vilka uppgifter som ska behandlas och vad de ska användas till. Den personuppgiftsansvarige är skyldig att se till att behandlingen inte strider mot personuppgiftslagen.

- Ibland kan det vara svårt att avgöra vem som är personuppgiftsansvarig. Ett exempel är då kommuner ställer krav i upphandlingar på entreprenörer att använda positioneringssystem och leverera uppgifter från dessa till kommunen. Vem som är personuppgiftsansvarig i dessa fall beror på de faktiska omständigheterna. Faktorer som spelar in är till exempel vad som avtalats vid upphandlingarna och vilka möjligheter som entreprenörerna har att själva påverka hur positioneringssystemen utformas och används. Det är viktigt att de inblandade parterna, innan systemen tas i drift, fastställer vem som är personuppgiftsansvarig i dessa fall och att detta tydliggörs för de som berörs.
- Positioneringssystem köps ofta som en tjänst från en utomstående leverantör. Det kan innebära att leverantören behandlar personuppgifter för arbetsgivarens räkning, till exempel om de lagras på en server hos leverantören. Arbetsgivaren måste då i egenskap av personuppgiftsansvarig upprätta ett skriftligt avtal – ett så kallat biträdesavtal – med leverantören. I avtalet ska det föreskrivas att leverantören får behandla personuppgifterna bara i enlighet med instruktioner från arbetsgivaren och att leverantören är skyldig att vidta lämpliga tekniska och organisatoriska åtgärder för att skydda uppgifterna. Biträdesavtalet kan utgöra en del av ett annat avtal med personuppgiftsbiträdet, till exempel ett uppdragsavtal.



Tänk på att arbetstagare normalt inte kan samtycka

- Arbetsgivare kan i regel inte stödja sig på samtycken från arbetstagarna till den behandling av personuppgifter som aktualiseras vid användningen av positioneringssystem. Det beror på att arbetstagare ofta befinner sig i en beroendeställning gentemot sina arbetsgivare och därför inte kan lämna sådana frivilliga samtycken som personuppgiftslagen kräver.
- Om de anställda erbjuds rimliga alternativ och inte utsätts för någon direkt eller indirekt påtryckning att välja ett system baserat på positioneringsteknik kan det vara tillåtet för arbetsgivaren att behandla personuppgifter med stöd av samtycken från de anställda. Ett sådant exempel är körjournalshantering, där de anställda kan välja mellan manuellt ifylld körjournal och ett system som bygger på positioneringsteknik.
- Arbetsgivare som vill använda positioneringssystem måste normalt stödja sig på en intresseavvägning. Arbetsgivarens intresse av att utföra behandlingen måste då väga tyngre än de anställdas intresse av skydd mot intrång i den personliga integriteten. Vid den helhetsbedömning som ska göras i dessa fall bör bland annat följande faktorer vägas in:
 - ändamålen med behandlingen
 - hur uppgifterna hanteras och hur resultatet används
 - vilken information som ges till de anställda
 - om behandlingen kan utföras på ett mindre integritetskänsligt sätt
 - vilken teknisk och administrativ säkerhet som finns för uppgifterna
 - förekomsten av fackliga överenskommelser och innehållet i dessa och
 - om behandlingen följer god sed på arbetsmarknaden.

* Om en operatör är direkt inblandad, till exempel genom att erbjuda positionering via GSM-nätet kan även lagen (2003:389) om elektronisk kommunikation (LEK) gälla. Post- och Telestyrelsen (PTS) utövar tillsyn enligt den lagen. För mer information om LEK, se PTS webbplats: www.pts.se.

Precisera ändamålen med behandlingen

- Innan ett positioneringssystem tas i drift måste det tydligt ha bestämts för vilka ändamål personuppgifter ska behandlas. Ändamålen bör skrivas ned. Det är till exempel vanligt att arbetsgivare anger säkerhetsskäl som motiv för att använda positioneringssystem. Det ska då tydligt framgå om det är personalens säkerhet som avses eller någon annan form av säkerhet. Det ska också framgå vilka kontroller av de anställda som kan bli aktuella.
- Uppgifter som har samlats in för vissa ändamål får inte senare användas för andra, oförenliga ändamål. Uppgifter som samlats in för säkerhetsändamål får till exempel inte senare användas för prestationsmätning av anställda.
- Uppgifterna i positioneringssystemet måste ha faktisk betydelse för de ändamål som bestämts med behandlingen. Arbetsgivaren måste bland annat ta ställning till om ändamålen med behandlingen motiverar att den utförs på individnivå. Om ändamålet till exempel är att föra statistik är det tillräckligt att samla in uppgifter på ett sådant sätt att enskilda inte kan identifieras.
- Ändamålen ska vara förenliga med god sed. På arbetsmarknaden är detta något som bland annat bestäms vid diskussioner mellan arbetsmarknadens parter. Parterna behöver överväga i vilken utsträckning man ska få övervaka anställda. Till exempel ska det kanske gå att stänga av systemet på arbetstagarens fritid.

Spara inte uppgifter längre än nödvändigt

- Det är ändamålen med behandlingen som styr hur länge uppgifterna får bevaras. Innan systemen tas i drift måste därför arbetsgivaren ta ställning till hur länge uppgifterna behöver sparas utifrån de bestämda ändamålen. Om systemet till exempel används för arbetsledning i realtid är det sällan motiverat att spara uppgifterna annat än under mycket kort tid.
- Om arbetsgivaren vill använda uppgifterna för statistikändamål och därför spara dem under en längre tid ska uppgifterna avidentifieras. När uppgifter inte längre kan kopplas till enskilda personer gäller inte personuppgiftslagen.

Ge tydlig information till de anställda

- Arbetsgivaren måste informera personalen i förväg om personuppgifter behandlas i positioneringssystem och måste också se till att det finns väl fungerande rutiner för detta. Datainspektionen rekommenderar att informationen sprids aktivt till de anställda, både skriftligt och muntligt innan systemet börjar användas. Informationen bör även finnas lättåtkomlig, till exempel på intranät eller i personalpärm.
- Informationen till de anställda ska vara tydlig och utförlig. Det ska framgå vem som är personuppgiftsansvarig för behandlingen (normalt arbetsgivaren), ändamålen med behandlingen, vilka kategorier av uppgifter som samlas in, hur länge uppgifterna sparas och om uppgifterna lämnas ut till utomstående (till exempel ett företag som sköter driften av systemet). De anställda ska också upplysas om sin rätt att få veta vilka uppgifter som finns registrerade om dem (registerutdrag) och om möjligheten att få eventuella felaktigheter rättade.

Skydda personuppgifterna

- Tillgången till uppgifterna i positioneringssystemen måste begränsas med hjälp av ett system för behörighetsstyrning så att endast personer som behöver åtkomst för att kunna utföra sitt arbete har det. Åtkomsten bör begränsas tekniskt så mycket som det är praktiskt möjligt med hänsyn till den aktuella verksamheten och känsligheten hos personuppgifterna. Det måste finnas väl fungerande administrativa rutiner om hur systemen får användas. Inloggningen ska vara individuell för att kunna följa upp felaktig eller obehörig åtkomst.
- Det måste finnas enlogg (det vill säga en historik över vem som loggat in och vad man gjort i systemet) samt rutiner för regelbunden uppföljning av loggen, för att kunna utreda felaktig eller obehörig användning av personuppgifter i systemet. Loggen måste skyddas mot otillåtna ändringar. De anställda ska informeras om att loggning och logguppföljning sker.
- När personuppgifter från positioneringssystem överförs via öppna nät, som exempelvis Internet, bör uppgifterna skyddas med hjälp av kryptering.

Det här får arbetsgivaren göra

Det är normalt **tillåtet** att med stöd av en intresseavvägning enligt personuppgiftslagen använda positioneringsteknik för följande ändamål:

- logistik och fördelning av resurser
- säkerhet
- framställning av statistik och
- klagomålshantering och kundservice.

För att behandlingen ska vara tillåten krävs naturligtvis att den sker i överensstämmelse med personuppgiftslagen. Behandlingen måste till exempel vara sakligt motiverad i verksamheten och får inte utföras på ett alltför närgånget eller omfattande sätt.

Det här får arbetsgivaren inte göra

Det är normalt **otillåtet** att med stöd av en intresseavvägning enligt personuppgiftslagen använda positioneringssystem för följande ändamål:

- Rutinmässig kontroll av arbetad tid. Detta är endast tillåtet undantagsvis vid konkret misstanke om allvarligt missbruk av arbetsgivarens förtroende, till exempel missbruk av tidredovisningen.

Kontakta Datainspektionen

E-post: datainspektionen@datainspektionen.se Webb: www.datainspektionen.se
Tfn 08-657 61 00. Postadress: Datainspektionen, Box 8114, 104 20 Stockholm.