Sammanfattning – Dataskyddsförordningen

Framtagen i samarbete mellan branschföreningarna Hyreskedjan och Swedish Rental

Inledning

Den 25 maj 2018 träder den nya dataskyddsförordningen i kraft i hela Europa.
Denna sammanfattning riktar sig till företag som är anknutna till Swedish Rental och Hyreskedjan. Det är en vägledning till dej som är verksam inom maskinuthyrningsbranschen. Våra företag påverkas främst av hur vi behandlar personuppgifter i verksamheten.

Bakgrund till förordningen

Ett bakomliggande syfte med den nya förordningen har varit att skapa ett **utökat skydd** för rätten till ett **privatliv** som ytterst regleras i *EU:s rättighetsstadga – artikel 8.* Där står bland annat följande:

- Varje individ har rätt till skydd av de **personuppgifter** som rör individen.
- Personuppgifter skall behandlas lagenligt för **bestämda** ändamål och bygga på antingen den personens **samtycke** eller **lagenlig grund**. Varje individ har dessutom rätt att få **tillgång** till alla insamlade uppgifter som rör denne och att få **rättelse** av dem i de fall det finns felaktigheter.
- En oberoende **myndighet** ska kontrollera att dessa regler följs. I Sverige är det Datainspektionen som har ansvar för detta.

Den nya dataskyddsförordningen skall gälla lika för alla länder inom EU vilket gör att det inte är tillåtet med begränsningar eller undantag på landnivå. Då förordningen är helt ny och ännu ”oprövad” så kommer det med all sannolikhet att växa fram ett antal tolkningar och prejudikat på hur företag, myndigheter och organisationer skall tillämpa förordningen rent praktiskt.

Personuppgifter
Det kan i sammanhanget vara värt att påpeka att en personuppgift inte enbart är detsamma som en individs person-, eller samordningsnummer. Definitionen på en personuppgift är betydligt bredare än så.
En personuppgift är all sorts information som kan knytas till en enskild individ. Exempel på sådan information är förutom det som nämnts ovan;

- namn
- adress till bostad/sommarstugan
- mailadress
- IP nummer
- fast telefon och mobilnummer som kan knytas till en viss person oavsett om ett abonnemang står på en privatperson eller ett företag
- foton på en individ
- registreringsnummer på privatägt fordon
- ljudinspelningar på en individ
- bolagsnummer för de som har handelsbolag eller enskilda firmor

Känsliga personuppgifter
I dataskyddsförordningen skiljer man på personuppgifter och känsliga personuppgifter. De sistnämnda kräver ytterligare och restriktioner för att säkerställa ett skydd till individen. Exempel på känsliga personuppgifter är:

- ras/etniskt ursprung
- åsikter/tillhörighet när det gäller religion
- politisk tillhörighet
- sexuell läggning
- facklig tillhörighet
- medlemskap i ideella organisationer/föreningar
- uppgifter om hälsotillstånd (allergier)

Grundläggande principer som personuppgiftshanteringen bygger på
Alla personuppgifter skall behandlas på ett lagligt, korrekt och öppet sätt så att den registrerade förstår hur dennes uppgifter behandlas och vad syftet är.
Personuppgifter får endast behandlas om ett tydligt syfte finns och de får enbart behandlas kopplat till angivet syfte och aldrig för andra ändamål.
Enbart personuppgifter som är nödvändiga för ändamålet får användas. Det handlar om ”need to have” och inte ”nice to have” som princip.
Lagringstiden av personuppgifter skall vara så kort som möjligt. Personuppgiftsansvarig måste dessutom säkerställa att alla data om den registrerade kan raderas.
Slutligen har personuppgiftsansvarig skyldighet att säkerställa relevant skydd av personuppgifter.

Ansvarsroller

I den nya dataskyddsförordningen definieras några roller inom som har ett ansvar vad gäller hantering av personuppgifter.

Personuppgiftsansvarig (PUA)

Personuppgiftsansvarig likställs med en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen (se nedan) och medlen för behandling av personuppgifter. Det betyder i klartext att alla företag är personuppgiftsansvariga oavsett om de är enskilda firmor eller juridiska personer som aktiebolag. Den personuppgiftsansvarige har ansvar för alla personuppgiftsbehandlingar denne utför oavsett om det sker i egen regi eller med hjälp av biträde (se nedan). Vidare ska personuppgiftsansvarig kunna redogöra och påvisa att denne följer den nya dataskyddsförordningen.

Personuppgiftsbiträde (PUB)

Personuppgiftsbiträde är en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning. Alla som på ett eller annat sätt hjälper ett företag där någon form av personuppgifter utväxlas är alltså biträden enligt denna definition.
Det är ganska många biträden som på ett eller annat sätt är knutna till varje företag gällande personuppgiftshantering. Vi lever i en IT baserad värld där mycket och förvisso alltmer går ut på att integreras vilket betyder att en mängd uppgifter utbyts mellan både företag och myndigheter. Det handlar om IT företag som anlitas för olika ändamål; datadrift, datalagring, nätverk, web lösningar med mera. Andra exempel är företag som hjälper till med fakturering, skanning av leverantörsfakturor, löneadministration. Vidare omfattas Skatteverket (tar bland annat emot kontrolluppgifter), Försäkringskassan, Arbetsförmedlingen, Pensionsförvaltningsbolag. Listan går att göra lång.
Förordningen ställer ett antal krav på personuppgiftsbiträden som de är skyldiga att följa. Det krävs också att så kallade biträdesavtal upprättas. Avtalet ska finnas mellan personuppgiftsansvariga bolag och de företag/organisationer (personuppgiftsbiträden) som hjälper företag med olika tjänster där personuppgifter registreras.

Dataskyddsombud

Dataskyddsombud är en person eller organisation som ska ha sakkunskap om datalagstiftningen och förfaranden. Ombudet bistår den personuppgiftsansvarige och/ eller personuppgiftsbiträdet för att övervaka den interna efterlevnaden av dataskyddsförordningen och andra dataskyddsbestämmelser.
Myndigheter och statliga organ är skyldiga att tillsätta dataskyddsombud. Vidare omfattas även företag vars ”kärnverksamhet” går ut på att hantera mycket personuppgifter såsom exempelvis resebyråer, sjukhus, rekryteringsbolag, lönehanteringsföretag och försäkringsbolag.

När får personuppgifter samlas in och bearbetas?
Den nya förordningen ger en tydlig fingervisning om att alla företag, myndigheter och organisationer i första hand skall söka efter andra identifieringslösningar än de som är kopplade till en personuppgift. Genom att förebygga och ersätta med andra id lösningar ökar det privata skyddet. Det innebär även att antalet personuppgifter som behöver lagras och hanteras minskar. Vad gäller själva reglerna runt insamling av personuppgifter så finns följande att notera för det stöd som krävs enligt den nya förordningen:

- Personuppgifter får endast samlas in för **särskilda**, uttryckligen berättigade **ändamål**. Det krävs således ett uttryckligt syfte. Det ska finnas en rimlig förklaring till varför just personuppgift används och inte en annan kodlösning.
- Det måste finnas en **rättslig grund**.

Kan företaget styrka dessa två kriterier kan man använda personuppgifter i sin verksamhet.

Rättslig grund
Det finns flera sätt att åberopa rättslig grund.

- **Rättsliga förpliktelser**. Inom vissa områden är företag skyldiga att registrera personuppgifter t.ex. gällande inlämning av kontrolluppgifter till Skatteverket, uppgiftslämning och lagerhållning enligt bokföringslagen med mera.
- **Avtal**. I vissa fall är det berättigat för företaget att hantera personuppgifter när det hänger ihop med att företaget har tecknat någon form av avtal såsom anställningsavtal, kund- och leverantörsavtal med kontaktuppgifter
- **Samtycke**. Ett företag kan inhämta samtycke från en person för att hantera dennes personuppgifter. Företaget måste vara tydlig med att specificera vilka personuppgifter som samtycket avser. Det ska vara lätt för en utomstående t.ex. en granskande myndighet att verifiera ett samtycke i efterhand. En person kan när som helst kan återkalla ett samtycke. Det innebär att företaget då omgående måste sluta använda dennes personuppgifter samt garantera att de uppgifter som finns lagrade om personen tas bort.
- **Intresseavvägning**. Slutligen är det möjligt att åberopa rätten till att använda personuppgifter om företaget kan hävda att dess intresse är större än den enskildes rätt till privatliv. Det kan t.ex. gälla i marknadsföringssyften via utskick på mail, sms eller bli kontaktad via telefon. Dock gäller att om den enskilde individen frånsäger sig att bli kontaktad igen så måste företaget säkerställa att så inte sker.

För att du som företag ska kunna bekräfta att du följer förordningen förväntas du dokumentera ner på vilka sätt du gör detta. Datainspektionen uttrycker en vilja att varje personuppgiftsansvarig kan uppvisa en lista över alla de personuppgiftsbehandlingar som sker i ditt företag och att du kan styrka ditt syfte(ändamål) samt vilken rättslig grund som du åberopar för att hantera varje typ av personuppgift.

Informationsplikten
Företaget som samlar in, bearbetar och lagrar personuppgifter har informationsplikt till den person som uppgifterna gäller. Det krävs således att företaget på lämpligaste sätt informerar den berörde om vilka uppgifter som det handlar om och vad syftet är. I de fall uppgifterna lämnas vidare till andra t.ex. försäkringskassa, arbetsförmedling, skattemyndighet, revisionsbyrå, pensionsförvaltare, försäkringsbolag ska den enskilde personen informeras även om detta.

Lagring av personuppgifter
Den nya förordningen är betydligt tuffare skriven vad gäller rätten att lagra personuppgifter. Lagstiftaren har önskat att begränsa den rättigheten för att på så vis ge ett utökat personskydd till varje individ. All lagring av personuppgifter måste kunna motiveras. Företaget behöver ange ett syfte samt hur lång tid som personuppgifterna behöver lagras.
En annan aspekt av lagring är att företaget måste kunna garantera att samtliga personuppgifter kan raderas när så erfordras. Detta gäller oavsett var personuppgifter är lagrade såsom; affärssystem, IT- serverar, web-/hemsidor, sociala medier som företaget är ansvarig över, läsplattor, bokningssystem, mobiler, arkiv etc. Detta gäller även personuppgifter som lagerförs i pärmar, mappar och dokumentskåp.
Det blir viktigt för varje företag att ha rutiner som gör att detta fungerar på ett tillfredsställande sätt. Ifrågasätt och minimera all lagerföring av personuppgifter.

Säkerhet och incidentberedskap
Alla som samlar in, behandlar och lagerhåller personuppgifter har ett stort ansvar att detta sker på ett säkert sätt. Uppgifterna ska garanteras ett ordentligt skydd mot utomstående. Det ska finnas lösningar som försvårar och så långt det är möjligt förhindrar att företaget släpper ifrån sig personuppgifter. Det kan ske till följd av misstag eller om företaget utsätts för ”hackare” som ändrar, förstör och/eller stjäl personuppgifter.
Ett krav i den nya dataskyddsförordningen är att så fort ett företag anser sig ha råkat ut för en personuppgiftsincident så har företaget en skyldighet att rapportera detta till datainspektionen. Det är då viktigt att påpeka att lagstiftaren är mycket tydlig i att alla typer av incidenter ska rapporteras. Det betyder således att en borttappad eller stulen mobiltelefon direkt kan bli föremål för just en sådan incidentrapport. Detta då det i telefonen finns personuppgifter eller möjligheter att komma in i något av företagets system.
Företaget har 72 timmar på sig att utreda en incident och bedöma skadans art innan det måste rapportera. Datainspektionen kommer inledningsvis sannolikt att få hantera en mycket stor incidentrapportering. Över tid kan vi förhoppningsvis se att det växer fram en praxis på vad som ska vara uppfyllt för att rapportskyldighet kan anses föreligga. I dagsläget ska alla typer av incidenter rapporteras.

Information om kunder i säljstödsprogram s.k. CRM system
Många företag använder så kallade CRM system för att dokumentera uppgifter runt sina kunder. Datainspektionen ställer krav på företag som har CRM system att utarbeta tydliga rutiner för detta.

Registrerades rättigheter
Den registrerade har rätt att få information om vilka personuppgifter som databehandlas av personuppgiftsansvarig. Det betyder att den registrerade har rätt till att begära ut ett registerutdrag som anger sådan information. Detta skall vara kostnadsfritt för den registrerade.

Vidare har den registrerade full rätt att åberopa att fel skall rättas och ofullständiga uppgifter kompletteras. Personuppgiftsansvarig har i sådana fall skyldighet att åtgärda samt att informera när åtgärderna är klara. Slutligen har den registrerade, som bland annat nämnts under avsnittet om lagring ovan, rätt att begära komplett radering av alla personuppgiftsbehandlingar om denne som inte kan motiveras på andra grunder såsom t.ex. rättsliga förpliktelser.
Datainspektionen ställer krav på att alla företag/myndigheter/organisationer ska kunna ta fram registerutdrag över samtliga personuppgiftsbehandlingar per individ. Det måste finnas rutiner för att rätta fel samt att radera information när det är relevant.

Tillsyn och sanktioner

Datainspektionen är som ovan nämnts tillsynsmyndighet i Sverige för att säkerställa att dataskyddsförordningen följs av företag, myndigheter och organisationer.
Inspektionen har ett antal verktyg till hjälp för att sköta sin roll. Dessa är:

- **Tillsyn.** Inspektionen har rätt att göra tillsyn genom att besöka företag, intervjua personal samt begära in uppgifter och information för att kunna göra en bedömning om aktuellt företag följer riktlinjerna i förordningen.
- **Föreläggande**. Datainspektionen kan fatta ett beslut om föreläggande vilket med all sannolikhet i detta fall kommer att handla om att aktuellt företag bedöms behöva vidta åtgärder för att följa förordningen.
- **Varning**. Datainspektionen kan också dela ut en varning till företag som i något avseende bryter mot reglerna.
- **Reprimand**. Det är en skarpare form än varning. Detta är en erinran /tillrättavisning med krav på omedelbar åtgärd och rättelse för företaget att vidta.
- Utfärda **administrativa sanktionsavgifter.** Datainspektionen kan fatta beslut om sanktionsavgifter. Syftet med denna avgift är att den ska vara effektiv, proportionell och verka avskräckande. Denna åtgärd kommer att vara en kompletterande del till ovan nämnda möjligheter för Datainspektionen att agera. I samband med att denna avgift skall fastställas så beaktar datainspektionen ett antal parametrar såsom antal personuppgifter, ändamål, vidtagna åtgärder för att minska intrång, tidigare överträdelser och samarbetsvilja.

Sanktionsavgifternas storlek

Den högre avgiften för företag är satt till max 20 MEUR eller 4 % av företagets globala omsättning. Den tillämpas om företaget kan anses ha brutit mot följande saker i förordningen:

- De grundläggande principerna i förordningen
- De registrerades rättigheter
- Överföring till tredje land (utanför EU)
- Underlåtenhet att rätta sig efter förelägganden, varning eller reprimand

Den lägre avgiften för företag är satt till max 10 MEUR eller 2 % av företagets globala omsättning. Den tillämpas om företaget kan anses ha brutit mot följande saker i förordningen:

- Inbyggt dataskydd
- Föra register över behandlingar
- Utse dataskyddsombud
- Vidta säkerhetsåtgärder
- Anmäla personuppgiftsincident

Företagen kan överklaga beslut som Datainspektionen har fattat till Förvaltningsrätten.

Den registrerades möjligheter

En individ kan själv vidta åtgärder utöver att kontakta aktuellt företag och begära rättelser. Det går även att lämna klagomål direkt till Datainspektionen.

Källor:

- *Datainspektionens utbildningsmaterial daterat 30 januari 2018.*
- *Infograf från datainspektionen*
- *Dataskyddsförordningen, svensk version, General Data Protection Regulation (GDPR) 2016/679.*