För bilbranschens bästa

Nya dataskyddsregler om 25 maj 2018

Den 25 maj 2018 kommer EU:s dataskyddsförordning att börja gälla som lag i Sverige och ersätter då personuppgiftslagen (PUL).

Här kommer en första information om vad de nya reglerna innebär för företag inom bilbranschen. Denna information är långt ifrån heltäckande och det återstår även i dagsläget en del obesvarade frågor från både från Regeringen och Datainspektionen (DI). MRF kommer givetvis följa utvecklingen och underhand återkomma med mer information i frågan. Informationen (som baserar sig på Datainspektionens info) är tänkt att vara en inledande checklista när ni ska ta reda på vilka de viktigaste skillnaderna är mellan den nuvarande lagstiftningen och den nya dataskyddsförordningen och hur de påverkar er.

Många av dataskyddsförordningens begrepp och principer går att återfinna i nuvarande PUL. Om ni och t.ex. er generalagent redan idag har väl genomarbetade åtgärder och rutiner för att säkerställa att personuppgiftslagen följs, så kommer ni att ha en bra grund att utgå från. Det är dock viktigt att poängtera att dataskyddsförordningen även innehåller stora förändringar och vissa helt nya bestämmelser.

Ändringarna är i korthet följande:

För privatpersoner:

- Ökad insyn gällande vilka personuppgifter som företaget hanterar
- Lättare att flytta sin information - t.ex. mellan sociala nätverk och eller leverantörer
- Rätt att invända mot att personuppgifterna används för direktmarknadsföring
- Rätt att invända mot att personuppgifterna används för automatiserat beslutsfattande och profilering
- Lättare att klaga - om uppgifter hanteras felaktigt hos Datainspektionen
- Rätt att bli glömd från t.ex. kundregister, sökmotorer och webbplatser

MRF, Box 5611 (Karlavägen 14A, 1tr), 114 86 Stockholm
Telefon +46 8 701 63 00 **E-post** mrf@mrf.se **Hemsida** www.mrf.se

För företag:

- Skyldighet att kunna visa att förordningen följs, vilket kan medföra
- Krav på ökad dokumentation
- Sanktionsavgift på upp till 20 miljoner euro eller 4 procent av organisationens omsättning när en organisation missköter sin behandling av personuppgifter

Förberedelser inför nya dataskyddsförordningen

1. **Vilka personuppgifter hanterar ni**?

Gå igenom och dokumentera vilka personuppgifter ni hanterar, hur de samlas in och till vem uppgifterna lämnas ut. Ni kan behöva göra en bred översyn för att ta reda på vilka uppgifter som hanteras inom de olika delarna av er organisation. Om ni dokumenterar detta kan det hjälpa er att uppfylla dataskyddsförordningens krav på att ni måste kunna visa att förordningens bestämmelser följs. Andra sätt att uppfylla detta krav att införa en policy för dataskydd och tydliga rutiner vid hanteringen av personuppgifter.

2. Vilken information lämnar ni till den registrerade?

Ni bör kontrollera den information som ni lämnar till de registrerade och fundera över vilka förändringar av den informationen som kan bli nödvändig att göra. Bland annat kommer ni att behöva informera om den rättsliga grunden för behandlingen, hur länge personuppgifterna lagras och möjligheten att lämna klagomål till tillsynsmyndigheten (som i Sverige är Datainspektionen) om man anser att ens personuppgifter har hanterats felaktigt av er. Här kommer MRF att införa en standardskrivning i MRF:s leveransvillkor och reparationsvillkor.

3. Hur skall ni tillmötesgå den registrerades rättigheter?

I stort sett kommer de registrerade att ha samma rättigheter som i dag, men rättigheterna förstärks med dataskyddsförordningen. Därför bör ni se över era rutiner för att säkerställa att ni kan uppfylla alla rättigheter som de registrerade har gällande:

- få tillgång till sina personuppgifter
- få felaktiga personuppgifter rättade
- få sina personuppgifter raderade
- invända mot att personuppgifterna används för direktmarknadsföring
- invända mot att personuppgifterna används för automatiserat

- beslutsfattande och profilering
- flytta personuppgifterna (dataportabilitet)

Dataskyddsförordningen innehåller i likhet med PUL en skyldighet att på begäran lämna information till de registrerade om vilka uppgifter som behandlas om dem.

4. Med vilket rättsligt stöd behandlar ni personuppgifter?

De rättsliga grunderna för behandling av personuppgifter är i stort sett oförändrade. Ni kan därför redan nu kartlägga vilka behandlingar ni genomför och med vilken rättslig grund ni gör detta.

En viktig fråga är vilken rättslig grund vi idag har för att hantera kunders personuppgifter som lämnas i samband med köp och reparationer av bilar. De rättsliga grunder vi har idag i bilbranschen är i huvudsak genom avtal. Dessa grunder kommer även finnas kvar i det nya direktivet. Viktigt är däremot att tänka på att uppgifter utan den registrerades samtycke endast får ske om behandlingen är nödvändig för att ett ändamål som rör ett berättigat intresse hos den personuppgiftsansvarige, om detta intresse väger tyngre än den registrerades intresse av skydd mot kränkning av den personliga integriteten. Detsamma gäller om behandlingen är nödvändig för att tillgodose ett berättigat intresse hos en tredje man som personuppgifterna ska lämnas ut till. Det berättigade intresset kan normalt anses föreligga inom bilbranschen när det gäller återförsäljare och verkstäder möjligheter att för att kunna komma kontakt med ägaren eller brukaren i samband med underhåll, reparationer, viktiga uppdateringar m.m. Eventuellt kommer framöver denna intresseavvägning behöva kodifieras i en för bilbranschen gemensamt ”code of conduct” som kommuniceras med DI. Ni bör dokumentera även era slutsatser för att ni också ska kunna visa att ni uppfyller dataskyddsförordningens krav.

5. Hur inhämtar ni samtycke?

Enligt ovan behövs normalt med stöd av avtal (underskrivet köpeavtal eller arbetsorder) inget samtycke för att behandla de väsentliga personuppgifter som efter en intresseavvägning är nödvändiga för att hålla kontakt och informera kunden i olika sammanhang. Däremot kan ibland inhämtning av personuppgifter ske på andra sätt t.ex. vid olika intresseanmälningar, provkörningar m.m. och om uppgifterna skall även används i direktmarknadsföring från samarbetspartners etc. Då måste vara fråga om en frivillig, specifik

och otvetydig viljeyttring genom (precis som idag enligt PUL) vilken den registrerade, efter att ha fått information, godtar behandlingen av personuppgifterna. Det får inte råda någon tvekan om att den registrerade godtar behandlingen av personuppgifter. Till exempel godtas inte ett tyst samtycke eller en på förhand ikryssad ruta på en webbplats. Om ni stödjer er på samtycke för att behandla personuppgifter behöver ni försäkra er om att kraven på samtycke i förordningen är uppfyllda. Om så inte är fallet, måste ni antingen förändra era rutiner eller finna en annan rättslig grund för behandlingen.

För bilbranschens bästa

6. Vad ska ni göra vid personuppgiftsincidenter?

Ni måste dokumentera alla sådana händelser. När det inte är osannolikt att incidenten medför risker för enskildas fri- och rättigheter måste ni anmäla händelsen till tillsynsmyndigheten inom 72 timmar**.** Om incidenten kan leda till att personer utsätts för allvarliga risker såsom diskriminering, id-stölder, bedrägerier eller finansiella stölder ska ni även informera de registrerade om händelsen så att de kan vidta nödvändiga åtgärder.

7. Har ni byggt in skydd för personuppgifter i era IT-system?

Ni bör redan nu ta hänsyn till dataskyddsförordningens regler när ni tar fram nya IT-system eller förändrar befintliga. Det ger en större möjlighet att följa reglerna, höja säkerheten och förhindra onödiga framtida kostnader.

8. Vem ansvarar för dataskyddsfrågor i organisationen/företaget

Vem skall vara personuppgiftsombud? Ett personuppgiftsombud är en person som ser till att personuppgifter behandlas på ett korrekt och lagligt sätt inom den egna organisationen. Personuppgiftsombudet kan jämföras med en internrevisor som påpekar fel och brister till den som är personuppgiftsansvarig. När man har utsett ett personuppgiftsombud anmäler man det till Datainspektionen.

David Norrbohm
Förbundsjurist MRF