Tips & Råd- GDPR

Bekräftelsekriteriet

Ditt företag måste kunna bekräfta att du följer förordningen. Det innebär att det *inte* räcker att bara tala om att du följer förordningen. Du måste också visa att du följer den genom att dokumentera hur personuppgiftshanteringen sköts i företaget. Följer du nedanstående råd uppfyller du bekräftelsekriteriet.

Överväg behovet av personuppgifterna

Börja med att kritiskt överväga vilka personuppgifter som du anser att du måste hantera i företaget och som inte kan ersättas med annan typ av identifiering. Ju mindre personuppgifter desto mindre att komma ihåg och hantera. Individens personliga skydd ökar om du minskar antalet personuppgiftsregistreringar.

Undvik känsliga personuppgifter

Generellt sett är vårt råd till företag inom maskinuthyrningsbranschen att vara mycket restriktiva i att registrera och lagerhålla känsliga personuppgifter. Det som anses vara känsliga personuppgifter är till exempel sexuell läggning, hälso-/sjukuppgifter, politisk tillhörighet, religionsuppfattning men även föreningstillhörighet och facklig organisation.

Personuppgiftsbehandlingar

Lista alla personuppgiftsbehandlingar som sker i företaget. Ange syfte (ändamål) med varje behandling samt vilken rättslig grund som du åberopar för att hantera varje typ av personuppgift. Till din hjälp finns ett exempel på hur du kan göra i B**ilaga 1** – Personuppgiftsbehandlingar. Försök hitta en rättslig förpliktelse eller att det finns ett avtal som föranleder behandlingen. Undvik samtycke i den mån det går eftersom det är betydligt mer jobb att hantera och hålla informationen uppdaterad.

Information till berörda

Glöm inte att informera alla registrerade om vilka uppgifter som används och varför. Informera också i de fall uppgifter lämnas till tredje part; skattemyndighet, pensions-förvaltare etc. Ta fram en lämplig form för att informera via hemsida/webshop, i kundavtal, i anställningsavtal, på fakturor, på ordersedlar, på uthyrningsdisken i depån samt muntligt där så är lämpligt.
Exempel på text gällande anställda: *”Jag som anställd vid xx tillåter att bilder på mig (i tjänst och i vissa fall ihop med mitt namn) kan komma att användas i företagets broschyrer, hemsida, sociala medier och interna blad. (Om jag har kundorienterade arbetsuppgifter kan viss information om mig vara tillåten att publicera ändå).”*

Hantering och korrigering av personuppgifter

Ange var dina personuppgifter finns lagrade. Utarbeta rutiner tillsammans med de personalbiträden som sköter hanteringen över hur alla typer av personuppgifter skall kunna identifieras, rättas, kompletteras och tas bort i rätt tid på rätt sätt.
Den som är registrerad har rätt att begära ut ett registerutdrag beträffande vilka personuppgifter som finns om individen samt var de finns lagrade. Vidare har individen rätt till att all information är korrekt. Underlätta detta arbete med funktioner i dina affärssystem t.ex. för uthyrning, fakturering, löneadministration som gör att du kan ta fram registerutdrag. Säkerställ också att det går att se vid vilken tidpunkt en uppgift har blivit rättad, kompletterad eller raderad.

Lagring av personuppgifter

All lagring av personuppgifter måste vara motiverad utifrån rättslig grund och ändamål. De får enbart lagras under en rimlig tid kopplat till ändamålet. Sätt därför upp ett regelverk för lagerhållning av personuppgifter. Nedan exempel kan fungera som exempel för att bygga en praxis:

- Rensa och kassera (på säkert sätt) bokföringsmaterial som är inaktuellt - för närvarande ska 7 år plus innevarande verksamhetsår finnas tillgängligt
- Uppgifter om anställda som slutat – max 1 år efter sista aktivitet
- Kunder som ej varit aktiva – max 1 år efter sista aktivitet
- Mobiltelefon, dator och läsplattor som byter individ – snarast efter telefonbyte
- Foton tagna på personer i samband med en mässa – snarast efter mässans slut
- Garantitid på en produkt eller ett åtagande – snarast efter garantitidens utgång
- Produktskada/försäkringsärende – snarast efter att skadan är färdigreglerad

Biträdesavtal

Lista ned alla företag, myndigheter och organisationer som på ett eller annat sätt biträder ditt företag i hantering av personuppgifter. När du har listat ner detta skall du teckna ett biträdesavtal med var och en av dem. Se förslag på avtalsmall med personuppgiftsbiträden i **Bilaga 2 –** Personuppgiftsbiträdesavtal.

Policy

Säkerställ att det finns en Dataskyddspolicy inkl. cookiepolicy på företaget. I **Bilaga 3** – Dataskyddspolicy finns en mall som hjälper dej med detta.

Riskbedömning - säkerhet

Gör en riskbedömning över områden där de största riskerna kan finnas att ditt företag drabbas av personuppgiftsincidenter. Det innebär att analysera i vilka lägen det finns risker för att obehöriga kan komma åt de personuppgifter som ni hanterar på ert företag. Det gäller interna och externa samt fysiska och digitala intrång av obehöriga personer.

Prioritera de områden som kan ge störst skada för de registrerade. Vidta relevanta förebyggande åtgärder. Tänk både på de tekniska och organisatoriska åtgärderna som behöver göras till exempel:

- behörigheter (rutiner för när personer slutar/ändrar befattning i företaget)
- hanteringen av lösenord på företaget (inga fusklappar i närheten av datorn)
- lösenordets sammansättning (små/stora bokstäver, siffror, specialtecken)
- låsta utrymmen (skåp eller rum med lås där ett fåtal behöriga personer har tillgång)
- larm (för att minska risken för inbrott)
- galler för fönster på bottenvåningen (lätt att bara krossa en ruta och ta en telefon/dator/läsplatta som ligger framme)
- hantering av stulna/borttappade telefoner/datorer/läsplattor
- placering av server och hantering av backup

CRM - system

Vår rekommendation till de företag som har CRM system är att utarbeta tydliga rutiner. Säkerställ även att CRM systemet innehåller så få personuppgifter som möjligt för att minimera risken att bryta mot förordningen.

- Vilka personuppgifter är det verkligen nödvändigt att vi lagrar i vårt CRM system?

- Vilka personuppgifter som berör t.ex. intresseområden, smak, storlek, familjeförhållande, födelsedagar, hälsoläge etc. kan motiveras för att sköta kundrelationen?
- Hur ska vi säkerställa rättslig grund för att få registrera alla uppgifter? I detta fall är det mycket sannolikt att ett personligt samtycke krävs.
- Hur säkerställer vi då att vi har koll på alla samtycken över tid så att de är aktuella och uppdaterade?
- Hur säkerställer vi att uppgifter som inte längre skall lagerföras tas bort?

Personuppgiftsincident

Var noga med att rapportera *personuppgiftsincidenter* till Datainspektionen. I detta läge rapportera alla incidenter där risk föreligger att personuppgifter kan röjas. Ditt företag har 72 timmar på sig att utreda och ta beslut om rapportering. Tänk dock på att det mycket sällan går att utesluta att personuppgifter finns i t.ex. mobiler, i bärbara datorer eller på läsplattor i det fall de blir stulna eller kommer på villovägar.
Datainspektionen kommer 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.

* * * * * *