# Checklista – GDPR-anpassning av NPS-program

När din verksamhet genomför undersökningar kopplade till ett NPS-program (eller andra former av undersökningar) så hanteras det i regel en mängd personuppgifter. Här kommer en övergripande checklista med punkter som kan vara bra att se över i god tid innan GDPR ersätter PUL den 25 maj 2018. Då ska allt redan finnas på plats.

## 1. Vilka personuppgifter hanteras och vad är syftet med behandlingen?

Gå igenom vilka personuppgifter som hanteras i samband med NPS-programmet och fastställ syftet med behandlingen. Ställ dig frågan vilka uppgifter som verkligen är nödvändiga att behandla för att uppfylla syftet? Gör en avvägning mellan nytta och nöje. Behandla ingen information som inte är relevant. Beskriv vad som motiverar behandlingen av personuppgifterna.

## 2. Var hanteras personuppgifterna och av vilka?

Se över vilka enheter och verksamheter, både internt och externt, som berörs av behandlingen inom NPS-programmet. Vilka datorer, mobiler, system etc. Vilka leverantörer, samarbetspartners och andra berörs? Hur är säkerheten för behandlingen av data, och var sker behandlingen? Se över om ni behöver vidta några säkerhetsåtgärder för att se till att behandlingen är säker och korrekt för att minimera risken att incidenter kan inträffa. Identifiera var servrar står som hanterar data. Är det någon server som finns utanför EG/EES-området? Se till att överföringen av data till och från samarbetspartner/leverantör är identifierad och säkrad.

Gör en översiktskarta som visar hur, vad och vem som hanterar data för varje enskild situation. Översiktskartan bör även innehålla kontaktuppgifter till de som berörs av hanteringen.

## 3. För register över behandlingen

Din verksamhet behöver föra ett översiktligt register som har med alla de behandlingar som sker hos företaget. Information som bör framgå av registret är till exempel, företag och organisationsnummer, kontaktuppgifter till ansvarig kontaktperson, typ av register, vilka uppgifter som behandlas, syftet med behandlingen, gallringsrutiner, vilka aktörer som berörs av hantering av personuppgifter.

## 4. Ta fram gallringsrutiner för behandlingen

Det är vanligt att personuppgifter inom ett NPS-program behöver sparas så att det finns möjlighet att följa resultat över tid och se om kunden har förändrat sina åsikter och rekommendationsgrad till verksamheten allteftersom utveckling och förbättringar skett. För alla undersökningar som genomförs är det trots det viktigt att ha satt en gallringsrutin för behandlingen i det enskilda fallet. Om data inte behöver sparas ska de gallras enligt den rutin som ni fastställer för den enskilda undersökningen.

## 5. Mallar, rutiner och processer vid förfrågningar och incidenter

Ta fram mallar, rutiner samt processer så att ni vet vad som behöver göras, hur det ska göras när ni får en förfrågan från en kund som har fått en undersökning och vem som ansvarar för att agera. Det finns olika förfrågningar som kan komma, så det är bra att ha rutiner på plats för de olika scenarios som kan dyka upp. Hur sker registerutdrag, vem får göra det, vad krävs för underlag för att göra det etc? Hur sker rättning av fel, får rättningen några följdeffekter på andra ställen? Hur sker radering/blockering? Får det några följdeffekter på andra ställen? Om det inträffar en säkerhetsincident, till exempel ett dataintrång eller en oavsiktlig förlust av uppgifter - har ni ett incidenthanteringsteam som tar hand om detta? Vem kontaktar Datainspektionen inom 72 timmar från det att det inträffar? Hur och när informeras de som drabbas av incidenten?

## 6. Se över avtal

Finns det avtal som tar upp personuppgiftshantering utifrån GDPR-perspektiv med alla leverantörer, samarbetsparters och övriga som kan komma att hantera personuppgifter i form av Personuppgiftsbiträde till er? Här gäller det att göra en inventering över vilka avtal som finns och inte finns för att komplettera där det saknas avtal.

## 7. Action-hantering med respekt och varsamhet

Har ni kopplat på direktuppföljning av kundupplevelser i ert NPS-program är det viktigt att respektera respondenten och visa hänsyn. Följ upp varsamt och tacka för värdefull information.

## 8. Intern information och kunskap

Alla som berörs av hanteringen behöver få information och kunskap om hanteringen i enlighet med GDPR så att de kan följa de regler som gäller från och med maj 2018.

## 9. Vilken information behöver den som tar emot en undersökning få?

En av de allra viktigaste punkterna. Värna och respektera den vars personuppgifter det är som behandlas. Det gäller att tydligt informera om all hantering som sker. Informationen ska framgå i inbjudan till undersökningen. Till exempel är det viktigt att ha med information om vilket syfte undersökningen har och därmed syftet med behandlingen av personuppgifterna, om undersökningen är anonym eller inte, om det kommer att överföras data till annan part, om företaget kan komma att kontakta respondenten och följa upp svaren efter deltagandet. Denna information ska vara synlig före det att den som får inbjudan klickar på länken till undersökningen.

Informationen ska vara fullständig till mottagaren av undersökningen. Det innebär bland annat att det ska framgå vem som skickar ut undersökningen, vem som behandlar informationen, hur den behandlas och vilka rättigheter mottagaren har i samband med hanteringen. Upprätta därför en personuppgiftspolicy som anger detta. Denna ska finnas tillgänglig för respondenten i inbjudan till undersökningen. Det är tillräckligt att lägga policyn i en länk i inbjudan.

I samband med att respondenten aktivt klickar på länken/undersökningsknappen för att delta godkänner denne behandlingen.

**Checklistan är inte fullständig, utan din verksamhet kan behöva se över fler saker och områden för att GDPR-säkra verksamheten. Lycka till med ditt GDPR-arbete för ditt NPS-program. Tveka inte att höra av dig till oss om du vill ha ett bollplank kring dessa frågor!**

Johan Laudon
johan@marketdirection.se
070-743 77 83
www.marketdirection.se

MarketDirection™
Experts in NPS - Growth through customer loyalty