POLICY
PERSONUPPGIFTSHANTERING
2024-12-09

1. ALLMÄNNA UTGÅNGSPUNKTER

Mangold omfattas av EU:s dataskyddsförordning, GDPR, som reglerar hur personuppgifter får behandlas. Mangold har därför en policy som ska säkerställa en säker hantering av personuppgifter och en efterlevnad av GDPR.

2. ANSVARIGA

CEO är i egenskap av företrädare för Mangold ytterst ansvarig för att kraven som åligger Mangold som personuppgiftsansvarig efterlevs.

Inom Mangold finns det även ett utsett Dataskyddsombud (DPO) som ansvarar för att övervaka att Mangold fullföljer skyldigheter och krav stipulerade i GDPR samt andra rättsliga förpliktelser.

Alla chefer i verksamheten ansvarar för att deras avdelning följer de rutiner och riktlinjer som styrelse och CEO har fastställt, samt att alla nya eller förändrade behandlingar av personuppgifter meddelas DPO.

3. DEFINITIONER

3.1. Personuppgift

En personuppgift är varje uppgift som avser en identifierad eller identifierbar fysisk person. Avgörande är att uppgiften, enskilt eller i kombination med andra uppgifter, kan knytas till en levande person. En personuppgift kan till exempel vara namn, bild, telefonnummer eller depånummer.

3.2. Känsliga personuppgifter

Vissa personuppgifter är till sin natur särskilt känsliga och har därför ett starkare skydd enligt GDPR. Känsliga personuppgifter är till exempel sådana som avslöjar en persons etniska ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller uppgifter om hälsa och sexualliv. Även personuppgifter som rör lagöverträdelser och personnummer är att betrakta som känsliga. Utgångspunkten är att det är förbjudet att behandla sådana personuppgifter. Det finns dock flera undantag från förbudet.

3.3. Behandling av personuppgifter

Med behandling av personuppgifter avses en åtgärd eller en kombination av åtgärder beträffande personuppgifter. En åtgärd kan vara insamling, lagring, användning, läsning eller radering av en personuppgift eller annat som innebär hantering av personuppgifter.

På Mangold behandlas ett flertal personuppgifter på många olika sätt av olika funktioner. Rådgivare behandlar personuppgifter om kunder, medan HR behandlar personuppgifter om anställda. Compliance behandlar personuppgifter om både kunder och anställda.

3.4. Personuppgiftsansvarig och dataskyddsombud

En personuppgiftsansvarig är den fysiska eller juridiska personen som ensam eller tillsammans med någon annan är ansvarig, samt bestämmer ändamålen och medlen för behandlingen av personuppgifter.

Den som behandlar personuppgifter (likt i Mangolds fall) måste i vissa fall utse ett dataskyddsombud. Ombudets roll är att kontrollera att dataskyddsförordningen följs inom organisationen.

Mangold har gjort bedömningen att för den verksamhet som Mangold bedriver så krävs inte ett dataskyddsombud enligt lag. Mangold ska dock följa samtliga lagar och regler och på ett kontinuerligt och riskbaserat sätt arbeta med dataskyddsfrågor i enlighet med denna policy, för att säkerställa att detta arbete sker effektivt har Mangold beslutat att ett dataskyddsombud ändå ska utses.

3.5. Principer för behandling av personuppgifter

När en behandling av personuppgifter sker måste uppgifterna behandlas på ett *lagligt*, *korrekt* och *öppet* sätt. Det är även viktigt att personuppgifterna skyddas från otillåten behandling eller ändring, samt att integritet och konfidentialitet säkerställs. De tre principerna för behandling av personuppgifter innebär följande.

- *Laglighet*: Personuppgifter ska inte behandlas på ett sätt som strider mot förordningen. Exempelvis ska personuppgifter inte användas för ett annat ändamål än för det som de samlades in.
- *Korrekthet*: De personuppgifter som samlas in ska vara korrekta och uppdaterade.
- *Öppenhet*: Behandlingen av personuppgifter ska vara öppen och transparent, vilket innebär att det ska vara tydligt vilka personuppgifter som behandlas, hur de behandlas och varför de behandlas. Information om behandlingen måste lämnas till den registrerade på ett klart och tydligt sätt.

3.6. Ändamålsbegränsning

Personuppgifter får endast samlas in för särskilda, uttryckligt angivna och berättigade ändamål. Den som samlar in och behandlar personuppgifter måste därför innan insamling bestämma varför uppgifterna samlas in. Personuppgifterna får inte senare användas i något annat syfte än det som de ursprungligen samlades in för.

3.7. Uppgiftsminimering

I linje med att personuppgifter endast får samlas in för särskilda, uttryckligt angivna och berättigade ändamål ställs även ett krav på uppgiftsminimiering, nämligen att uppgifterna som samlas in ska vara adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka de behandlas.

Detta innebär att Mangold aldrig ska inhämta fler uppgifter än vad som krävs för att uppnå de ändamål som är grund för behandling av personuppgifter, samt löpande rensa bort uppgifter när dessa inte längre behövs med hänsyn till ändamålen som var grunden till att de behandlades.

3.8. Lagring av personuppgifter

Den personuppgiftsansvariga får inte förvara personuppgifter i en form som gör att de registrerade kan identifieras under en längre tid än vad som är nödvändigt för det ändamål som personuppgifterna behandlas. Personuppgifter som inte längre behövs för det ändamål de samlades in ska därför tas bort eller avidentifieras.

För att säkerställa att personuppgifter inte sparas längre än nödvändigt bör den som behandlar personuppgifter införa tidsfrister och rutiner för radering eller avidentifiering. Varje chef på Mangold ansvarar för att sådana rutiner fastställs inom deras respektive avdelningar och ansvarsområden.

4. PERSONUPPGIFTSHANTERING

4.1. När personuppgift får behandlas

För att få behandla personuppgifter krävs en *laglig grund* för behandlingen. Vad som är en laglig grund bestäms i artikel 6 i Dataskyddsförordningen. Ett eller flera av de berättigade villkoren måste alltså vara uppfyllda för att en personuppgift ska få behandlas.

Laglig grund kan vara samtycke, avtal, skyddande av intresse av grundläggande betydelse, rättslig förpliktelse, myndighetsutövning eller uppgift av allmänt intresse, eller intresseavvägning.

”Skyddande av intresse av grundläggande betydelse” samt ”myndighetsutövning eller uppgift av allmänt intresse” kan Mangold aldrig använda som grund för behandling.

4.2. Den registrerades rätt att få information om behandlade personuppgifter

Den registrerade har rätt att få en bekräftelse från den personuppgiftsansvarige om att dennes personuppgifter behandlas. Den registrerade har rätt att få tillgång till personuppgifterna och information om bland annat ändamålen med behandlingen, vilka kategorier av personuppgifter det gäller och hur länge personuppgifterna ska sparas. Den registrerade har alltså rätt att få tillgång till de personuppgifter som rör dem själva, men inte själva dokumentet eller mailet där dennes personuppgifter behandlas.

Mangold sammanställer denna information på en särskild del av hemsidan; www.mangold.se/GDPR och registrerade hänvisas i första hand till denna sida för information om hur deras personuppgifter behandlas.

4.3. Rättelse och radering

Enligt dataskyddsförordningen ska den personuppgiftsansvarige *rätta* felaktiga personuppgifter om den registrerade begär det. Den personuppgiftsansvarige ska även *radera* personuppgifter om den registrerade begär det förutsatt att vissa villkor är uppfyllda. Om en personuppgift rättas eller raderas måste den personuppgiftsansvariga informera alla mottagare av personuppgiften om att uppgiften har ändrats eller raderats.

Det finns dock bestämmelser i andra lagar som gör att radering på begäran av den registrerade inte ska göras i alla situationer. Exempelvis enligt lagen om värdepappersmarknaden måste värdepappersbolag spara vissa uppgifter i minst fem år, detsamma gäller enligt penningtvättslagen medan bokföringslagen stipulerar en lagringstid om sju år. Därutöver finns den generella preskriptionstiden för att väcka talan i domstol om tio år, vilken kan berättiga lagring under den tiden. Sådan lagring är tillåten enligt dataskyddsförordningen eftersom det finns undantag i andra lagar.

4.4. Personuppgifter från eller till någon annan än den registrerade

Om personuppgifter erhålls från någon annan än den registrerade måste den registrerade informeras om att dennes personuppgifter kommer att behandlas. Information om behandlingen måste skickas inom en månad från det att man fick del av uppgifterna. Om den personuppgiftsansvarige tror att denne själv kommer att skicka personuppgifterna vidare till en tredje part måste den registrerade informeras om detta senast när personuppgifterna lämnas ut första gången.

Om personuppgifter är tänkta att överföras till ett tredje land måste den registrerade lämna sitt samtycke till detta. Om den personuppgiftsansvarige, innan en affärsrelation inleds, vet att den registrerades uppgifter kommer att överföras till ett tredje land måste den personuppgiftsansvarige berätta det för den registrerade.

4.5. Förteckning över personuppgiftsbehandling

Personuppgiftsansvariga är skyldiga att föra ett register över all personuppgiftsbehandling inom företaget. Dessa register ska upprättas skriftligen, vara tillgängliga i elektronisk format och hållas uppdaterade. På begäran ska registret göras tillgängligt för Integritetsskyddsmyndigheten.

5. PERSONUPPGIFTSBITRÄDE

Personuppgiftsbiträde är den som behandlar personuppgifter för en personuppgiftsansvarigs räkning. Ett personuppgiftsbiträde finns alltid utanför den personuppgiftsansvariges organisation. Ett personuppgiftsbiträde kan vara en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ.

De biträden som den personuppgiftsansvarige anlitar ska kunna ge tillräckliga garantier för att behandlingen uppfyller kraven i dataskyddsförordningen och säkerställer att den registrerades rättigheter skyddas.

Ett personuppgiftsbiträde och dess personal får enbart behandla personuppgifter enligt instruktion från den personuppgiftsansvarige. Biträdet får inte anlita ett annat biträde om inte biträdet på förhand fått ett skriftligt tillstånd av den personuppgiftsansvarige.

Även personuppgiftsbiträdet kan bli föremål för tillsyn eller administrativa sanktionsavgifter och bli skadeståndsansvarig.

Vidare måste den personuppgiftsansvarige och personuppgiftsbiträdet upprätta ett så kallat biträdesavtal. Dataskyddsförordningen räknar upp vad ett sådant biträdesavtal ska innehålla.

6. DATASKYDDSOMBUD

Mangold har valt att utse ett dataskyddsombud (DPO). Mangold ska se till att DPO inte har uppgifter som kan leda till intressekonflikter. Detta innebär särskilt att DPO inte kan inneha tjänst inom organisationen som innebär att DPO fastställer ändamålen med och medlen för behandling av personuppgifter. DPO ska ha en självständig ställning när denne utför sitt uppdrag.

Mangold ska säkerställa följande:

1. Att DPO regelbundet inbjuds att delta i möten på högsta och mellanliggande förvaltningsnivå.
2. Att DPO deltar när beslut med följder för dataskyddet fattas.
3. Att DPOs åsikt i relevanta frågor ges tillbörlig vikt. Om Mangold väljer att inte följa DPOs råd ska detta dokumenteras.
4. Att DPO ska informeras och rådfrågas omedelbart när en personuppgiftsincident har eller kan ha inträffat.
5. Att DPO har resurser i former av information, tid och utbildning för att kunna genomföra sitt uppdrag.

6.1. DPO:s uppgifter

DPO ska informera och ge råd till Mangold om personuppgiftesbehandling. DPO ska även kontrollera efterlevnaden av GDPR. Det kan innebära att DPO:

1. Samlar in information om hur personuppgifter behandlas inom Mangold.
2. Analyserar och kontrollerar om personalen följer bestämmelserna fastslagna i denna policy och GDPR.
3. Utfärdar rekommendationer till Mangold om personuppgiftsbehandlingen.

Anställda, kunder och andra registrerade ska lätt kunna komma i kontakt med DPO. För kunder och andra externa registrerade sker kontakt via post till adressen:

Mangold Fondkommission AB
Att: GDPR
BOX 55691
102 15 STOCKHOLM

DPO ska agera kontaktperson gentemot Integritetsskyddsmyndigheten.

Om verksamheten vill föreslå ändringar i denna policy eller någon annan policy som berör Mangolds behandling av personuppgifter ska DPO rådfrågas innan ändringen läggs fram för beslut, för att säkerställa att föreslagna ändringar inte negativt inverkar på Mangolds arbete med att leva upp till kraven i GDPR.

6.2. Personuppgiftsincidenter

Utredning av incidenter hanteras av COO och Compliance i enlighet med bestämmelser i policy för incidenthantering och väsentliga händelser. Dessa avdelningar ansvarar för att hålla DPO informerad om personuppgiftsincidenter och de åtgärder som vidtas.

DPO ska vara behjälplig med råd och stöd om det inträffar eller kan ha inträffat en personuppgiftsincident. DPO ska dokumentera den potentiella personuppgiftsincidenten och den bedömning som har gjorts därav, samt tillställa Compliance och COO denna bedömning.