

Policy för GDPR och personuppgiftshantering



Innehållsförteckning

1	INLEDNING OCH SYFTE	2
2	TILLÄMPNING OCH REVIDERING	2
3	ORGANISATION OCH ANSVAR	2
4	BEGREPP OCH FÖRKORTNINGAR	3
5	PERSONUPPGIFTSBEHANDLING OCH LAGLIGA GRUNDER	4
5.1	Anställda	4
5.2	Rekrytering	4
5.3	Kunder	6
5.4	Kontaktpersoner i projekt	7
6.	RUTINER VID BEHANDLING AV PERSONUPPGIFTER	7
6.1	Hantering av e-post	7
6.2	Hantering av Molntjänst	9
6.3	Hantering av papper och pärmar	10
6.4	Konsekvensbedömning	10
6.5	Lagringsminimering, arkivering och gallring	10
6.6	Registerutdrag	10
7.	KONTAKTUPPGIFTER	11

1 INLEDNING OCH SYFTE

Syftet med denna policy är att säkerställa att Currentum med tillhörande dotter- och systerbolag hanterar personuppgifter i enlighet med EUs dataskyddsförordning (General Data Protection Regulation – GDPR). Policyn omfattar alla behandlingar där personuppgifter hanteras och omfattar såväl strukturerad som ostrukturerad data.

I flera fall när vi begär in personuppgifter gör vi det i syfte att uppfylla lagstadgade eller avtalsenliga krav eller krav som är nödvändiga för att ingå avtal med exempelvis en anställd, en kund eller leverantör. Det handlar också om att vi ska kunna fullgöra ett uppdrag där kontakt med intressenter, projektledare eller andra berörda individer förekommer. I fall där den registrerade inte tillhandahåller de uppgifter som vi begär kan det i vissa fall medföra att vi inte kan ingå ett avtal eller fullgöra våra förpliktelser i ett avtal med den registrerade.

Denna policy är förankrad hos alla våra medarbetare.

2 TILLÄMPNING OCH REVIDERING

Styrelsen ansvarar för att behandlingen av personuppgifter följer denna policy. Policyn ska fastställas av styrelsen och uppdateras vid behov. VD är ansvarig för att hålla i processen kring årlig uppdatering av policyn till följd av nya och förändrade regelverk.

Denna policy är tillämplig för företagets styrelseledamöter, VD, medarbetare samt uppdragstagare som berörs av vår verksamhet.

3 ORGANISATION OCH ANSVAR

VD har det övergripande ansvaret för innehållet i denna policy samt att den implementeras och efterlevs av verksamheten. VD får delegera ansvaret och implementationen till lämplig person på företaget. VD har rätt att delegera implementering av denna policy till av denne utsedd utförare.

Alla medarbetare ansvarar för att de agerar i enlighet med denna policy och vad den vill säkerställa.

4 BEGREPP OCH FÖRKORTNINGAR

Begrepp	Betydelse
Personuppgift	En personuppgift är all slags information som direkt eller indirekt kan hänföras till en fysisk person som är i livet.
Registrerad	Den som en personuppgift avser, det vill säga den fysiska person som direkt eller indirekt kan identifieras genom personuppgifterna i ett register.
Personuppgiftsbehandling	En åtgärd eller kombination av åtgärder beträffande personuppgifter – oberoende av om de utförs automatiserat eller ej – såsom insamling, registrering, organisering och strukturering.

5 PERSONUPPGIFTSBEHANDLING OCH LAGLIGA GRUNDER

- Varje personuppgiftsbehandling ska ske enligt följande principer:
 - Laglighet
 - Ändamålsbegränsning
 - Uppgiftsminimering
 - Korrekthet
 - Lagringsminimering
 - Integritet och konfidentialitet

5.1 Anställda

Vilken är den lagliga grunden för behandlingen?

De anställdas personuppgifter inhämtas för att kunna fullgöra vissa skyldigheter enligt lag och/eller för fullgörande av enskilda avtal. De personuppgifter som behandlas är främst namn, personnummer, telefonnummer, bankuppgifter, underlag för ersättning och förmåner, adress, erfarenhet och utveckling, frånvaro, sjukdom och rehabilitering och i vissa fall information om närstående. De som mottar informationen är Löneadministratör, Närmsta chef, VD samt myndigheter när så krävs.

För vilka ändamål behandlas uppgifterna?

Personuppgifterna behandlas för bl.a. löneutbetalningar, beräkning av ersättning, lönerevision, tidrapportering, bonusersättning samt för kontakt av anhörig vid olycka. Informationen används också för granskning och utvärdering av prestation av den enskilde som ger ett underlag för utvecklingssamtal med den anställda. Informationen sparas också i syfte att säkerställa uppfyllelse av legala skyldigheter mot myndigheter.

Hur länge sparas uppgifterna?

Currentum AB ska aldrig lagra informationen längre än vad som är nödvändigt för ändamålet. Currentum AB genomför därför gallring av uppgifterna regelbundet.

5.2 Rekrytering

Vilken är den lagliga grunden för behandlingen?

För att Currentum AB ska kunna hantera ansökningar som den registrerade skickat in, genomföra intervjuer och sedan fatta beslut i ett rekryteringsförfarande måste Currentum AB behandla vissa personuppgifter. Grunden för denna behandling är intresseavvägning eller avtal.

Vilka uppgifter behandlas och vem är mottagaren?

Personuppgifter som behandlas av Currentum AB är bl.a. namn, födelsedatum, adress, e postadress, information om erfarenhet och färdigheter, fotografi m.m. De som tar emot uppgifterna är främst HR-chef eller VD.

För vilka ändamål behandlas personuppgifterna?

För att Currentum AB ska kunna hantera ansökningar, rekrytering och beslut om lämpliga medarbetare samlar vi in personuppgifterna.

Hur länge sparas personuppgifterna?

Currentum AB ska aldrig lagra informationen längre än vad som är nödvändigt ändamålen. Currentum AB genomför därför gallring av uppgifterna regelbundet.

5.3 Kunder

Vilken är den lagliga grunden för behandlingen?

För att Currentum AB ska kunna ingå avtal med kunder behandlar Currentum AB vissa personuppgifter vilka ofta är kontaktperson hos kundföretaget. Vissa personuppgifter behandlas också för att Currentum AB har en rättslig skyldighet, som exempelvis bokföringsskyldighet.

Vilka personuppgifter behandlas och vem är mottagaren?

Vi behandlar personuppgifter för kontaktpersoner i företag som vi har kundavtal med eller som vi förväntas få kundavtal med. Personuppgifter som behandlas kan exempelvis vara namn, telefonnummer, e postadress, personnummer eller andra ID som direkt eller indirekt kan knytas till personen. De som mottar uppgifterna är främst VD, ekonomiavdelning eller anställd som hjälpt till med affären eller på annat sätt bistått i säljarbetet.

För vilka ändamål behandlar vi personuppgiften?

I de fall ett kundavtal finns behandlar vi personuppgifter för att kunna fullgöra avtalet i sin helhet. Personuppgiften kan också behövas i samband med den dialog som kan förekomma innan ett avtal finns på plats. Företrädarens kontaktuppgifter kan också användas till att skicka offerter och erbjudanden om förslag till framtida affärsmöjligheter.

Currentum anlitar personuppgiftsbiträden för lagring av personuppgifter kopplade till kundavtal. Det kan röra sig om projektverktyg, bokföringsprogram eller molntjänster för lagring. Dessa personuppgiftsbiträden hanterar i dessa fall personuppgifter för vår räkning som personuppgiftsansvariga. I dessa fall har Currentum AB upprättat personuppgiftsbiträdesavtal för att garantera att personuppgifter behandlas på ett korrekt och säkert sätt.

Vissa leverantörer har valt att upprätta PuB avtal med Currentum för detta. Dessa redovisas i registerförteckningen under PuB avtal.

Hur länge lagras personuppgifterna?

Currentum AB ska aldrig lagra informationen längre än vad som är nödvändigt ändamålen. Currentum AB genomför därför i enlighet med intern policy gallring av uppgifterna regelbundet. Currentum AB kan dock behöva lagra personuppgifter efter att kundrelationen upphört i syfte att hantera avtalsrättsliga krav och/eller för att skicka erbjudanden som Currentum AB tror kan vara av intresse för före detta kunder. Personuppgifter sparas då en viss tid eller tills att personen inväntat mot vidare behandling. Personuppgifter kan också mer generellt behöva sparas för att uppfylla legala skyldigheter avseende bokföring. Personuppgifter sparas i dessa fall i upp till 8 år.

5.4 Kontaktpersoner i projekt

Vilken är den lagliga grunden för behandlingen?

Currentum anser att behandling av personuppgifter i syfte att fullgöra de åtagande som finns i vårt avtal med kund är viktigt. Vi använder oss således av en intresseavvägning för att i detta fall behandla personuppgifter inom ramen för uppdragens beskaffenhet.

Vilka personuppgifter behandlas och vem är mottagaren?

Vi behandlar i följande fall primärt namn, e-post, telefonnummer, adress och i vissa fall bild på personer.

För vilka ändamål behandlar vi personuppgiften?

För att Currentum ska kunna genomföra de projekt vi avtalat om med våra kunder krävs många olika kontakter såsom projektansvariga, arbetsgrupper, konsulter eller andra personer som agerar avtalsmässig part i projekt eller som på annat sätt kan bidra till projektens genomförande.

6. RUTINER VID BEHANDLING AV PERSONUPPGIFTER

- Våra uppgiftsbehandlingar dokumenteras löpande i *Personuppgiftsregistret*.
- Personuppgifter skall löpande rensas bort ur *personuppgiftsregistret* så snart syftet med behandlingen av personuppgiften är genomförd och avslutad.
- Uppföljning och utvärdering av vår hantering av personuppgifter ska ske årligen.
- Eventuella incidenter rörande personuppgifter som vi behandlar ska utan dröjsmål rapporteras till VD. VD ska utan onödigt dröjsmål och senast inom 72 timmar anmäla incidenten till Datainspektionen samt i övrigt vidta nödvändiga åtgärder med anledning av incidenten.
- Våra krav på att personuppgifter hanteras enligt GDPR ska alltid säkerställas vid upphandling och utveckling av IT-lösningar och tjänster, och ska vara en del i kravspecifikationen och eventuella avtal.

Currentum AB ska genomgående behandla personuppgifter på ett sådant sätt att vi undviker att kränka individers personliga integritet. I samtliga fall av personuppgiftsbehandling är Currentum mycket noga med att personuppgifter skyddas av lämpliga säkerhetsåtgärder. Currentum kommer att agera personuppgiftsansvarig och i vissa fall personuppgiftsbiträde och ovanstående principer ska gälla oavsett roll.

6.1 Hantering av e-post

Grundregel:

Hantering av personuppgifter ska främst ske i system, inte i e-post. Hantering av personuppgifter i e-post räknas också som behandling av personuppgifter och samma krav gäller som för alla andra behandlingar.

Alla medarbetare på Currentum är införstådda med att behandla e-post enbart till specifika ändamål inom ramen för sin tjänst. När en medarbetare skickar e-post ska hen tänka på att minimera antalet mottagare och innehåll som kan innebära oskälig behandling av personuppgifter.

Medarbetare ska heller inte lagra e-post som inte är relevant för tjänsteutövningen eller som inte direkt kan kopplas till pågående, kommande eller nyligen avslutade projekt. Denna typ av e-post ska löpande raderas från e-postservern för att på bästa sätt värna om den personliga integriteten hos de behandlade individerna.

Merparten av behandlingarna Currentum gör bygger på en intresseavvägning vilket innebär att vi vid varje enskilt tillfälle måste bedöma behandlingens relevans. I samband med att vi mottar e-post eller sänder e-post ska den vars personuppgifter behandlas få information om detta. Detta görs skriftligen i form av en hänvisning till Currentum policy om personuppgiftsbehandling som finns på Currentum hemsida. Om en individ motsätter sig behandlingen ska e- posten genast raderas.

Skicka aldrig känsliga eller skyddsvärda personuppgifter via e-post, till exempel uppgifter om någons hälsa, religiösa åskådning eller politiska åsikter. Skicka heller inga andra integritetskänsliga uppgifter som exempelvis lönekommentarer, värdering om en person eller någon typ av provresultat via e-post.

Använd systemet till att kommunicera, inte lagra uppgifter. Spara aldrig uppgifter i mail för att ”det kan vara bra att ha”. Osäkerhet kring en behandling ska föras vidare och diskuteras med den ansvarige för personuppgiftshanteringen.

6.2 Hantering av Molntjänst

Currentums företag som använder sig av molnleverantör. I de fallen lagras två typer av data som var och en vilar på två olika lagliga grunder för behandling.

- Kund- / Projektdata(Kunder)
- Interna dokument (Internt)

Personuppgiftsbehandling (Kunder) ska rensas vid avslutade projekt. Currentum har som mål att endast behandla personuppgifter i pågående projekt samt under garantitid men kan komma att av intresse för kund behöva spara projektuppgifter för framtida behov för att säkerställa service till kund. En avvägning av detta behov skall göras i samband med gallring. Koneos molntjänst ska vara den primära lagringsplatsen för all data kopplade till Kunder vilket gör att lagring lokalt på datorer, USB-stickor, i mail, i telefon eller på andra lagringsplatser icke specificerade i detta dokument skall undvikas. Currentum har som policy att lagring av personuppgifter i möjligaste mån ska ske på ett och samma säkert lagringsställe.

På lagringsplatsen/molntjänsten förekommer personuppgifter som lagras enligt en mappstruktur med behörighetsnivåer som ofta har en annan laglig grund för behandling, oftast avtalsmässig med syftet att säkerställa att Currentum kan fullgöra avtal med anställda, kommande rekryteringar, kunder eller leverantörer. Om ny undermapp läggs upp, som tidigare inte specificerats i personuppgiftsregistret, ska den anställde omedelbart ombesörja att registret uppdateras.

Generella krav vid hantering av personuppgifter i molnet:

- Lösenord för personlig åtkomst till dator, telefon och mejl ska ses som en värdehandling och bytas vid jämna mellanrum. Säkerheten på lösenordet är viktigt och unika sådana ska användas. Lösenord får inte skrivas ned i datorn eller på annat sätt delas med utomstående personer.
- Vid delning av mappar är det av yttersta vikt att ansvarig projektledare har full kontroll på vilka personer som har åtkomst till vilka mappar. Delning av mappar till utomstående personer ska sanktioneras av projektledare och utdelningen ska vara tidsbegränsad och i vissa fall åtkomstbegränsad beroende på känsligheten i de personuppgifter som behandlas i respektive kundmapp.
- Vid förlust av data eller vid misstanke om personuppgiftsläckage ska detta rapporteras till ansvarig för personuppgiftshantering omedelbart.
- Lagring av s.k. känsliga personuppgifter får aldrig lagras i molntjänsten utan samtycke och rapportering till ansvarig för personuppgiftshantering.

6.3 Hantering av papper och pärmar

Fysiska papper med personuppgifter ska enbart användas vid behov och så länge projekten är aktiva. Om möjligt ska sådan ostrukturerad data vara inlåst och ej tas hem eller föras utanför kontoret. När fysiska papper innehållande personuppgifter inte längre är relevanta för pågående projekt ska de rivas och/eller raderas.

6.4 Konsekvensbedömning

Vid personuppgiftsbehandling som sannolikt medför en hög risk för den registrerades integritet måste en konsekvensbedömning genomföras.

Syftet med bedömningen är att

- Förebygga risker innan de uppkommer
- Att bedöma om personuppgifter som samlas in är nödvändiga för ändamålet
- Att bedöma om den personuppgiftsansvarige har vidtagit tillräckliga åtgärder för att skydda den registrerades integritet och rättigheter.

Konsekvensbedömningen är ett av sätten för den personuppgiftsansvarige att påvisa sin efterlevnad.

6.5 Lagringsminimering, arkivering och gallring

En av de grundläggande principerna i dataskyddslagstiftningen är principen om lagringsminimering, det vill säga att samla in så få personuppgifter som möjligt. Du får bara samla in de uppgifter som behövs för att kunna utföra arbetet.

Det innebär i praktiken att när grunden för behandling upphör ska uppgiften arkiveras alternativt raderas. Grunden för behandling i projekt föreligger under projektets färdigställande och ytterligare tio (10) år.

6.6 Registerutdrag

Alla behandlade individer har rätt att få veta vilka personuppgifter Currentum behandlar. Vid fråga är vi skyldiga att översända ett registerutdrag som berör både strukturerat och ostrukturerat material. Dock gäller inte detta för utkast eller minnesanteckningar.

Ett registerutdrag ska innehålla:

- Ändamålen med behandlingen
- De kategorier av personuppgifter som behandlingen gäller
- De mottagare eller kategori av mottagare som personuppgiften har lämnats ut till
- Hur länge Currentum har för avsikt att behandla personuppgiften
- Att individen har rätt att begära radering av personuppgiften om den lagliga grunden för behandlingen så tillåter

- Rätten att inge klagomål till en tillsynsmyndighet
- Om uppgifterna inte kommer från den registrerade, varifrån då dessa uppgifter kommer

7. KONTAKTUPPGIFTER

Frågor om policy besvaras av ansvarig för personuppgiftshantering via info.sverige@currentum.se

Policy antagen av styrelsen för Currentum AB 2021-04-27