Policy för behandling av personuppgifter i Brain Accounting och Brain Competence

Syfte

Vi värnar om den personliga integriteten. Den som anförtror oss sina personuppgifter ska kunna känna sig trygg i att dessa hanteras på ett omdömesfullt och säkert sätt. Det gäller även våra kunder som inom ramen för våra uppdrag låter oss behandla personuppgifter för vilka de står som ansvariga. Därför har vi upprättat den här policyn. Den utgår från gällande dataskyddslagstiftning och utstakar riktlinjer för hur vi ska hantera avvägningen mellan den personliga integriteten, verksamhetens förutsättningar och annan tillämplig lagstiftning.

Syftet med den här policyn är dels att fastställa riktlinjerna för vårt interna arbete, dels att på ett transparant sätt visa våra intressenter hur vi behandlar personuppgifter. I slutänden handlar det om att skydda personuppgifter från att komma obehöriga tillhanda och om att underlätta för de som är registrerade att få reda på vilka uppgifter vi behandlar om dem samt att på ett enkelt sätt kunna radera dessa på begäran från den registrerade om och när lagstiftningen så tillåter.

Giltighet

Den Europeiska Dataskyddsförordningen (GDPR) trädde i kraft 25 maj 2018. Vi ser att innebörden av den i många fall kommer bli föremål för tolkningar och att praxis därför kommer att ändras över tiden. Vi ser också att införandet av den i vår typ av verksamhet, ett mindre företag som behandlar personuppgifter åt en stor mängd kunder med varierande kravställningar, inte kan vara fullständig från första dagen, utan successivt kommer att utvecklas i samförstånd med våra kunder. Därför kommer denna policy att uppdateras regelbundet. Den aktuella policyn är alltid den som finns på vår hemsida.

Denna version antogs av ledning och styrelse 1 juni 2018. Tidigare versioner upphör då att gälla.

Brain Accounting och Brain Competence

Brain är en av Sveriges ledande ekonomibyråer. Dotterbolaget Brain Competence arbetar med rekrytering och interimskonsulter inom ekonomi. Policyn omfattar båda bolagen som tillsammans benämns Brain. Vi hanterar personuppgifter både för egen och för våra kunders räkning. Brain har enbart juridiska personer som kunder. Det innebär att när vi i denna policy eller i tillhörande rutinbeskrivningar hänvisar till kunder eller potentiella kunder, så avses alltid juridiska personer. Brain är i vissa fall personuppgiftsansvarig (främst när vi behandlar personuppgifter för våra befintliga medarbetare, kandidater och interimskonsulter samt kontaktpersoner hos leverantörer, kunder och potentiella kunder) och i andra fall personuppgiftsbiträde (främst när vi behandlar personuppgifter för våra kunders anställda och kunder). Denna policy omfattar hur vi ska behandla personuppgifter i båda dessa roller.

Avtal med kunder och leverantörer avseende hantering av personuppgifter

I de fall vi agerar personuppgiftsbiträde åt våra kunder ska vi upprätta personuppgiftsbiträdesavtal. I de fall vi använder oss av leverantörer (främst systemleverantörer) som på något sätt behandlar eller har åtkomst till personuppgifter ska vi upprätta underbiträdesavtal. Våra kunder ska informeras om och godkänna användandet av underbiträden.

Skäl för behandling av personuppgifter

Vi behandlar inte personuppgifter i annat fall än när de behövs för att fullgöra verksamhetens syfte eller förpliktelser enligt avtal och lag. Vi ska vara noga med att motivera vilket skäl som föreligger för att vi behandlar en personuppgift. Här delar vi in detta enligt nedan:

- Lagkrav
- Avtalsmässiga åtaganden
- Verksamhetsmässiga skäl, s k intresseavvägning
- Samtycke från den registrerade*

* Vi sparar aldrig personuppgifter längre än vad som är motiverat av verksamhetens syfte eller förpliktelser enligt avtal och lag. Därför ser vi ingen situation där vi kommer att behöva inhämta samtycke för behandling av personuppgifter. Dock kan det uppstå situationer där större mängder av personuppgifter av administrativa skäl inte alltid kan raderas omedelbart efter det att verksamhetsmässiga syften och förpliktelser enligt lag och avtal har slutat gälla. I sådana situationer ska enskilda personuppgifter omedelbart raderas på begäran från den registrerade.

Vi behandlar följande typ av personuppgifter

En personuppgift är all information som direkt, eller indirekt, kan hänföras till en fysisk levande person. Nedan följer exempel på personuppgifterna vi behandlar. Vi kan i enskilda fall behandla andra personuppgifter utöver nedanstående.

- Namn
- Adress
- E-postadress
- Telefonnummer
- Ålder
- Födelsedatum
- Kön
- Titel
- Användarnamn och lösenord
- Fotografier
- Bankkontonummer och andra bankrelaterade uppgifter
- Löneuppgifter
- Uppgifter som har lämnats till oss i samband med rekryteringsprocesser, t ex utbildning och arbetslivserfarenhet

Särskilt känsliga personuppgifter

Vi behandlar generellt inte sådana personuppgifter som GDPR klassificerar som känsliga personuppgifter. Det kan dock i undantagsfall ske att vi i samband med specifika personalärenden, t ex rehabilitering eller andra arbetsrättsliga ärenden för våra anställda (då som personuppgiftsansvarig) eller för våra kunders anställda (då som personuppgiftsbiträde) behandlar känsliga personuppgifter. I de fall som behandlingen av sådana personuppgifter avviker från behandlingen av andra personuppgifter framgår det av denna policy.

Vi behandlar personuppgifter avseende följande grupper

Vi behandlar personuppgifter för en rad olika grupper av registrerade. I vissa fall gör vi detta som personuppgiftsansvarig, men de flesta personuppgifter behandlar vi i egenskap av personuppgiftsbiträde åt våra kunder. I de fall vi behandlar personuppgifter i rollen som personuppgiftsbiträde ska ett personuppgiftsbiträdesavtal upprättas med kunden. Det formella ansvaret för detta ligger hos kunden, men vi ska hjälpa till att ta fram avtal som är anpassade till vår specifika relation. Nedan beskrivs vilken typ av registrerade som vi behandlar personuppgifter för. Det kan i undantagsfall finnas personuppgifter som inte faller inom någon av nedanstående kategorier.

Anställda

Som personuppgiftsansvarig behandlar vi personuppgifter avseende våra anställda, det gäller främst de uppgifter som finns i ett normalt anställningsavtal, uppgifter avseende lönehantering samt uppgifter relaterade till HR, t ex underlag för individuell utveckling. Samtliga sådana uppgifter sparas aldrig längre än vad lagstiftningen kräver av oss. Det innebär bl a att HR-relaterade uppgifter raderas snarast efter det att en anställd har slutat.

Kandidater och interimskonsulter

Som personuppgiftsansvarig behandlar vi personuppgifter avseende potentiella anställda i Brain. Vi har tolkat det som att vi även är personuppgiftsansvarig när vi rekryterar eller förmedlar interimskonsulter till våra kunder. I detta fall är både vi och kunden personuppgiftsansvarig och därför ska inget personuppgiftsbiträdesavtal upprättas. Vi behandlar dels personuppgifter avseende personer som själv söker anställning hos oss eller våra kunder, dels personuppgifter som vi söker fram via LinkedIn. Personuppgifter som samlas in genom att kandidaten själv delger dem sparas så länge som det är verksamhetsmässigt motiverat, dock aldrig längre än två år efter det att de samlades in. Personuppgifter som samlas in via LinkedIn sparas i LinkedIns egna system och sparas därför aldrig längre än kandidaten väljer att tillgängliggöra dem på LinkedIn.

Kunder

Som personuppgiftsansvarig behandlar vi personuppgifter om kontaktpersoner hos våra befintliga kunder. Dessa personuppgifter behandlas aldrig på annat sätt än vad som kan motiveras med den pågående kundrelationen. Dessa personuppgifter sparas maximalt två år efter avslutad kundrelation.

Potentiella kunder

Som personuppgiftsansvarig behandlar vi personuppgifter om kontaktpersoner hos potentiella kunder. Dessa personuppgifter behandlas aldrig på annat sätt än vad som kan motiveras med en normal sälj- och marknadsbearbetning. I de fall dessa personuppgifter används för riktade utskick ska det på ett tydligt sätt framgå hur man kan avregistrera sig och när någon gör det, ska personuppgifterna raderas. Detsamma gäller om någon hör av sig till oss och begär att få sina personuppgifter raderade.

Leverantörer/partners

Som personuppgiftsansvarig behandlar vi personuppgifter om kontaktpersoner hos våra befintliga leverantörer/partners. Dessa personuppgifter behandlas aldrig på annat sätt än vad som kan motiveras med den pågående affärsrelationen. Dessa personuppgifter sparas maximalt två år efter avslutat samarbete.

Kunders anställda

Som personuppgiftsbiträde behandlar vi personuppgifter åt våra kunder som avser deras anställda. Detta sker främst i samband med att vi hanterar deras löner, men även i några fall i samband med HR-relaterade ärenden. Dessa personuppgifter behandlas aldrig på annat sätt än eller lagras längre än vad som krävs av avtalen med våra kunder eller av gällande lagstiftning.

Kunders kunder, medlemmar och bidragsgivare

Som personuppgiftsbiträde behandlar vi personuppgifter åt några av våra kunder som avser deras kunder, medlemmar och bidragsgivare. Sådana personuppgifter behandlas enbart i form av bokföringsunderlag och som medlems- och hyresgästförteckningar för bostadsrättsföreningar och fastighetsföretag. Dessa personuppgifter behandlas aldrig på annat sätt än eller lagras längre än vad som krävs av avtalen med våra kunder eller av gällande lagstiftning.

Behandling av personuppgifter

Nedan beskrivs våra riktlinjer för hur vi behandlar personuppgifter i varje steg från insamling till slutlig radering. För att säkerställa att riktlinjerna uppfylls i det dagliga arbetet har vi rutiner som beaktar och omfattar samtliga nedan angivna steg i behandlingen av personuppgifter. I tillämpliga fall skriver vi dessutom in rutiner för behandling av personuppgifter i den uppdragsbeskrivning vi har med respektive kund.

- Samla in och registrera
- Strukturera, organisera, bearbeta och använda
- Lagra och skydda
- Distribuera, överlåta och sprida
- Radera

Samla in och registrera

- Vi ska enbart samla in sådana personuppgifter som vi utifrån vår verksamhet är skyldiga att behandla enligt lag eller som kan anses ha väsentlig betydelse för att fullgöra våra befintliga åtaganden mot våra kunder och medarbetare så som vår verksamhet ser ut idag. Vi ska inte samla in personuppgifter i syfte att i framtiden använda dem till något annat än vad de är ämnade till idag.

- Enda undantaget till ovan är personuppgifter som syftar till att bedriva marknadsföring och försäljning mot personer i egenskap av befattningshavare i företag som finns inom vår målgrupp samt personuppgifter som kommer oss tillhanda i samband med rekrytering av personal.
- Vi ska aldrig samla in personuppgifter i syfte att direkt eller indirekt sälja dem.
- Vi bedömer utifrån punkterna ovan att vi inte i något fall behöver samtycke för att samla in de personuppgifter som vi behandlar och därför ska vi heller aldrig fråga om samtycke.
- Insamlingen av personuppgifter ska ske på ett sådant sätt att personuppgifterna snarast efter det att vi fått dem, ska överföras till de system eller den lagringsplats där de ska användas. Detta i syfte att säkerställa en säker lagring av personuppgifterna. Detta innebär att personuppgifter aldrig ska finnas kvar i mejl, webbformulär, fysiska papper eller motsvarande om dessa dokument inte kan anses utgöra en del av den långsiktiga lagringen av personuppgifter och att skyddet av personuppgifterna därmed är fullgott.

Strukturera, organisera, bearbeta och använda

- Vi använder enbart personuppgifter i sitt primära syfte, d v s i enlighet med de ändamål och skäl för vilka de ursprungligen samlades in eller överläts till oss. Dessa ändamål framgår i avtal eller annan typ av överenskommelse med våra kunder och medarbetare eller i rutindokument som i detalj styr användandet av specifika personuppgifter.
- I de fall vi strukturerar eller bearbetar personuppgifter görs detta aldrig med ett syfte eller på ett sätt som ändrar det ursprungliga ändamålet för användningen eller möjliggör att personuppgifterna analyseras på ett sätt som inte är förenligt med ändamålet.

Lagra och skydda

- Vi lagrar enbart personuppgifter där vi kan säkerställa att de har ett fullgott skydd. Det innebär följande:
    - Fysiskt material som innehåller personuppgifter förvaras inlåst i brandklassade skåp som enbart behörig person har åtkomst till.
    - Digital lagring på egen server skyddas av brandvägg från ledande tillverkare. Endast behörig personal har åtkomst till serverrummet.
    - Digital lagring i molnet sker enbart i ekonomisystem (och liknande) hos stora etablerade leverantörer med vilka vi har underbiträdesavtal som garanterar minst den säkerhet som motiveras av personuppgifternas art och de avtalsmässiga skyldigheter vi har i relation till våra kunder.
    - Personuppgifter ska inte lagras i mejl, utan snarast flyttas till relevant plats och därefter ska mejlet raderas.
- Antivirusprogram finns installerat på samtliga servrar och klienter. Antivirusdefinitioner uppdateras automatiskt dagligen.
- Åtkomsten av data (både från egen server och från de system som finns i molnet) styrs av behörigheter utifrån principen att ingen medarbetare ska ha tillgång till data som inte krävs för att vi ska kunna fullgöra våra skyldigheter mot kunder och myndigheter. Alla medarbetare har egen inloggning med lösenord som skapas och byts i enlighet med de rekommendationer som gäller för hög säkerhet.

Distribuera, överlåta och sprida

- Vi sprider eller överlåter aldrig personuppgifter till tredje part med undantag för vad vi enligt lag är skyldiga att rapportera in till myndigheter (t ex Skatteverket och Försäkringskassan) eller när vi i rollen som personuppgiftsbiträde har uppdrag av vår kund att göra det.
- Vi har i underbiträdesavtal med samtliga systemleverantörer, där vi använder molntjänster som kan innehålla personuppgifter som vi behandlar för vår egen eller för våra kunders räkning, säkerställt att de aldrig överlåter eller sprider några personuppgifter.
- Vi tolkar regelverket så att vi fortfarande kan distribuera personuppgifter till den registrerade eller till personuppgiftsansvarige (i de fall vi är personuppgiftsbiträde) via mejl. För att säkerställa ett högt integritetsskydd vid distribution av personuppgifter gäller dock följande:
    - Vi distribuerar aldrig s.k. känsliga personuppgifter via vanliga okrypterade mejl, utan använder då distributionsformer med högre säkerhet.
    - Vi distribuerar enbart i undantagsfall lönebesked via mejl (t ex engångslöner). Merparten distribueras via det lönesystem vi använder. För de allra flesta kunderna är detta Hogia Lön + och då använder vi Hogia MyPayslip som är en molnbaserad tjänst som uppfyller en hög säkerhet, väl i nivå med våra egna krav och vad vi har avtalat med våra kunder.
    - Vi undviker att mejla personuppgifter tillsammans med andra uppgifter för att underlätta för mottagaren att radera mejlet så fort personuppgifterna är sparade i enlighet med mottagarens riktlinjer.

Radera

- Vi ska alltid radera personuppgifter när de inte längre behövs för de skäl som de har samlats in och använts för. I många fall är vi dock beroende av att de system vi använder för behandling av personuppgifter är anpassade för att radera uppgifter på ett administrativt hanterbart sätt. Då flera system ännu inte är anpassade till detta, utgår vi just nu från följande riktlinjer för radering av personuppgifter för vilka de inte längre föreligger skäl att spara:
    - Alla sådana uppgifter ska raderas senast inom två år.
    - På begäran från personuppgiftsansvarig att radera en större mängd personuppgifter, ska detta göra så snart som det är administrativt möjligt, dock senast inom tre månader.
    - På direkt begäran från personuppgiftsansvarig eller från en registrerad att radera personuppgifter avseende en enskild registrerad ska uppgifterna raderas snarast, dock senast inom en månad.
    - Eventuella känsliga uppgifter ska raderas snarast.
- När vi avslutar uppdraget för en kund, och därmed vår avtalsmässiga skyldighet som personuppgiftsbiträde upphör, återlämnar vi alla personuppgifter till kunden eller till annan av kunden hänvisad part. Därefter raderas alla personuppgifter relaterat till uppdraget. I vissa fall kan delar av vår avtalsmässiga skyldighet kvarstå under en övergångstid. Det kan t ex gälla skyldigheten att rapportera in uppgifter till myndigheter. I sådana fall raderas personuppgifterna när denna skyldighet upphör.

Den registrerades rättigheter

Som registrerad innehar man ett antal rättigheter relaterade till hur personuppgifter behandlas. Nedan följder de rättigheter som har störst relevans för vår verksamhet och de personuppgifter som vi behandlar:

Rätt till information

Den registrerade har rätt att få information om vilka personuppgifter vi behandlar, ett s k registerutdrag.

Rätt till rättelse eller ändringar

Den registrerade har rätt att begära rättelse av felaktiga uppgifter eller ändra lämnade personuppgifter.

Rätt till återkallelse av samtycke

Vi använder oss i princip aldrig av samtycke som skäl att behandla personuppgifter. I de fall då detta eventuellt ändå har skett, så har den registrerade alltid rätt att återkalla detta samtycke och då raderar vi de personuppgifter som är insamlade med samtycke.

Rätt till radering under vissa omständigheter

Den registrerade har rätt att få sina uppgifter raderade i de fall vi har använt verksamhetsmässiga skäl, s k intresseavvägning som skäl för att behandla personuppgifter. Denna rätt gäller dock inte om vi t ex är skyldiga att behandla personuppgifterna enligt lag.

Notera att den registrerades rättigheter i vissa fall måste utövas mot den personuppgiftsansvariga som i sin tur säkerställer att vi som personuppgiftsbiträde vidtar relevanta åtgärder.

Övrigt

Denna policy kommer successivt att införas under 2018. Vi reserverar oss därför för att enskilda delar av denna policy eventuellt inte fullt ut är införda vid tidpunkten för denna versions ikraftträdande. Detta gäller dock inte de delar som avser säkerheten i hur personuppgifterna lagras och skyddas samt inte heller det som avser överlåtelse eller spridning.