Integritets- och dataskyddspolicy

För att säkerställa en god hantering av personuppgifter har PeopleAnalytics tagit fram en integritet och dataskyddspolicy som på ett konkret sätt ska upplysa kunderna om vilka uppgifter vi behandlar, varför samt hur länge de kommer att lagras samt vilka som kommer att ta emot dem.

Vid de tillfällen PeopleAnalytics tillhandahåller utbildningstjänster intar PeopleAnalytics ställningen som personuppgiftsansvarig för den eventuella behandling av personuppgifter som sker inför och under utbildningsuppdraget. Tjänsten tillhandahålls för att utbilda kunden och inte för att behandla kundens personuppgifter. Ändamålet med behandlingen av personuppgifter är att kunna tillhandahålla tjänsten och behandlingen utgör en förutsättning för att tjänsten ska kunna erbjudas. De uppgifter som samlas in och sparas är:

- För- och Efternamn
- Kontaktuppgifter såsom e-postadress, telefonnummer, arbetsplatsadress och yrkestitel
- Faktureringsuppgifter
- Anteckningar inför utbildningstillfällen
- Uppgifter om kostpreferens

Vid de tillfällen PeopleAnalytics tillhandahåller digitala tjänster intar PeopleAnalytics ställning som personuppgiftsbiträde. Detta beror på att kund, vid utnyttjandet av dessa tjänster, tillhandahåller bolagen med personuppgifter och bestämmer för vilka ändamål de får behandlas. För att säkerställa att behandlingen sker i enlighet med gällande personuppgiftslagstiftning skrivs alltid ett Biträdesavtal, se separat avtal. I tillägg till detta har vi en integritet och dataskyddspolicy vilket följande reglerar.

Denna bilaga anger minimikrav som EC PeopleAnalytics AB och i tillämpliga fall underbiträden följer avseende säker informationshantering vid leverans av tjänster för Kund som innefattar Behandling av Personuppgifter.

Du har rätt att invända mot att dina personuppgifter används för direktmarknadsföring. Med direktmarknadsföring avses alla typer av uppsökande marknadsföringsåtgärder, t.ex. via digitala utskick, e-post och sms. Du har rätt att kostnadsfritt motsätta dig att dina uppgifter används för sådana syften. PeopleAnalytics raderar uppgifter inom 14 dagar.

Allmänt om informationssäkerhet och integritet för PeopleAnalytics

PeopleAnalytics skyddar kunds information genom de säkerhetskontroller som anges i denna bilaga. Kommunikation med Kund gällande IT-incidenter eller andra tekniska frågor rapporteras till Kund enligt för ändamålet uppsatta rutiner.

Förlust/radering/förvanskning av Personuppgifter ska dessutom rapporteras till PeopleAnalytics Dataskyddsombud, Catrine Augustsson: catrine@peopleanalytics.nu

1. Informationssäkerhetspolicy

1.1 PeopleAnalytics har ett regelverk för informationssäkerhet som inkluderar en informationssäkerhetspolicy (integritetspolicy), vilken är fastställd och godkänd av ledningen och publiceras och kommuniceras till medarbetare och relevanta parter.

2. Organisation av informationssäkerhet

2.1 Det finns tydligt utpekade personer med ansvar för att upprätthålla en god IT-säkerhet.

3. Personalsäkerhet

3.1 PeopleAnalytics säkerställer att all personal med tillgång till Kunds

information skriver under bolagets sekretessavtal och kontinuerligt får utbildning i PeopleAnalytics informationssäkerhetspolicy.

3.2 PeopleAnalytics har en off-boardingprocess avseende personal som inkluderar borttagande av accessrättigheter, återlämning av IT-utrustning och underrättelse om fortsatta sekretesskrav.

4. Hantering av tillgångar

4.1 PeopleAnalytics ska behandla Kunds information som konfidentiell information.

4.2 Kommunikation av personuppgifter mellan kund och PeopleAnalytics ska hanteras av standardiserade fildelningstjänster

4.3 Kunds information behandlas och arkiveras logiskt separerad från PeopleAnalytics information och från information som tillhör andra.

4.4 Vid upphörande av PeopleAnalytics arbete för Kund ska PeopleAnalytics inom en månad på ett säkert och oåterkalleligt sätt tillse att Kunds information, inklusive eventuella kopior, raderas såvida inte ett sådant förfarande är oförenligt med gällande lagstiftning.

4.5 Om Kund önskar radera specifik personuppgift, antingen typ av uppgift eller vald person gör kunden det i portalen i inloggat läge.

5. Styrning av åtkomst

5.1 Användare får endast ges tillgång till information, informationsbehandlingsresurser, nätverk och nätverkstjänster som de specifikt beviljats tillstånd för.

5.2 Tilldelningen av konfidentiell autentiseringsinformation för åtkomst till Kunds information och informationsbehandlingsresurser styrs genom en formell hanteringsprocess.

5.3 Händelseloggar som registrerar användaraktiviteter skapas och bevaras i sådant skick att granskning kan utvisa vilken av Kunds information som blivit föremål för åtkomst, modifiering, obehörigt röjande eller destruktion.

6. Kryptering

6.1 Kryptografiska säkerhetsåtgärder används i enlighet med gällande avtal och författningar.

6.2 Kunds information skyddas av kryptografiska säkerhetsåtgärder vid överföring och lagring.

6.3 Kryptografiska nycklar ska hanteras centralt för att säkerställa skydd genom hela livscykeln.

7. Fysisk och miljörelaterad säkerhet

7.1 PeopleAnalytics servrar för PeopleInsights portalen finns placerade i Bromma utanför Stockholm. Servrarna hostas av Cubid som är en systemintegratör och tjänsteleverantör inom datasäkerhet, IP-kommunikation, virtualiserng och datalagring.

7.2 Fysisk åtkomst till Kunds informationsbehandlingsresurser (tillgång till serverhallar mm) är begränsad och kräver autentisering genom individuella ID-kort (eller motsvarande) samt pinkod.

7.3 Fysisk åtkomst till Kunds informationsbehandlingsresurser ska logga händelser så som datum, tid, ID-kort (eller motsvarande), dörr-id samt om åtkomst beviljats eller nekats.

7.4 Utrustning är placerade och skyddas för att minska riskerna för miljörelaterade hot och faror och möjligheter för obehörig åtkomst.

7.5 PeopleAnalytics sparar ingen kundrelaterade data som innefattar personuppgifter på ett ostrukturerat sätt utan all information lagras så att eventuell spårning kan genomföras enligt den rutinbeskrivning bolaget har.

8. Driftsäkerhet

8.1 Kraven om driftsäkerhet för att säkerställa korrekt och säker drift av Kunds informationsbehandlingsresurser gäller för leverantörer som tillhandahåller tjänster som stödjer Behandling av Kunds information i en driftmiljö.

8.2 PeopleAnalytics ska ha identifierat och upprättat en förteckning över information och informationsbehandlingsresurser som ingår i tjänsten.

8.3 Informationssystem har tillräcklig kapacitet för att säkerställa fortsatt tillgänglighet i händelse av en informationssäkerhetsincident.

8.4 Information och informationsbehandlingsresurser skyddas mot skadlig kod.

8.5 Det finns möjlighet till händelseloggar som registrerar användaraktiviteter (särskilt systemadministratörers och systemoperatörers aktiviteter), avvikelser, fel och informationssäkerhetshändelser.

8.6 Loggningsverktyg och logginformation skyddas mot manipulation och obehörig åtkomst.

8.7 Informationssäkerhetshändelser, så som exempelvis misslyckade inloggningsförsök, systemkrascher och ändringar av åtkomsträttigheter, registreras i loggar och inkludera information om datum, tid, användare, filnamn och IP-adress, där det är tekniskt möjligt.

8.8 Händelseloggar sparas i minst sex (6) månader och kan på begäran ställas till Kunds förfogande.

8.9 Säkerhetskopior (Back- Up) av information tas och testas för att säkerställa kontinuerlig och säker drift.

8.10 En process finns på plats för att säkerställa att uppdateringar (inklusive säkerhetsuppdateringar) eller kompenserande åtgärder, implementeras utan dröjsmål.

9. Kommunikationssäkerhet

9.1 Informationsbehandlingsresurser som innehåller Kunds information skyddas av brandväggar och övervakas för obehörig åtkomst.

9.2 Informationsbehandlingsresurser som används för åtkomst till Kunds information eller Kunds nätverk har säkerhetsmekanismer som skyddar mot obehörig avlyssning eller störningar genom brandväggar och andra system för att upptäcka och förhindra intrångsförsök.

10. Anskaffning, utveckling och underhåll av system

10.1 Utvecklings-, test- och driftmiljöer är separerade för att minska risken för obehörig åtkomst eller ändringar i driftmiljön.

10.2 Data från driftmiljöer där Kund data lagras får inte användas i test- och utvecklingsmiljöer utan att Personuppgifter avlägsnats eller anonymiserats. Vid speciella felsöknings- eller testuppdrag kan Kund data överföras till test- och utvecklingsmiljö under en begränsad tid för att därefter anonymiseras.

11. Leverantörsrelationer

11.1 Delning av Kundinformation med tredje part (underleverantörer) får bara ske efter skriftligt tillstånd från Kund och endast för de ändamål som anges i avtalet med Kund.

11.2 Underleverantörer får endast ges åtkomst till information som krävs för att uppfylla sina avtalsförpliktelser.

11.3 PeopleAnalytics skriver personuppgiftsbiträdes avtal med samtliga underleverantörer.

12. Hantering av informationssäkerhetsincidenter

12.1 PeopleAnalytics har rutiner för att säkerställa snabb, verkningsfull och korrekt hantering av informationssäkerhetshändelser.

12.2 PeopleAnalytics ska rapportera säkerhetshändelser som berör Kundinformation eller tjänster till Kund.

12.3 PeopleAnalytics ska samarbeta med Kund hanteringen av informationssäkerhetshändelser.
Samarbetet kan komma att innefatta åtkomst till bevis som lagras på exempelvis stationära eller bärbara datorer, nätverksservers, flyttbara lagringsmedia eller i säkerhetskopior.

13. Informationssäkerhetsaspekter avseende hantering av verksamhetens kontinuitet

13.1 Kraven om kontinuitet för att säkerställa kontinuerlig drift av Kunds informationsbehandlings-resurser gäller för leverantörer som tillhandahåller infrastrukturtjänster eller tjänster som stödjer Behandling av Kunds information i en driftmiljö.

13.2 PeopleAnalytics ska genomföra konsekvensanalyser och riskbedömningar (BIA/RA) för att identifiera risker som kan påverka leveransen av tjänsten till Kund.

13.3 Händelser som kan påverka leveransen av tjänsten till Kund ska registreras, analyseras och granskas av PeopleAnalytics och rapporteras till Kund

14. Efterlevnad

14.1 PeopleAnalytics genomför återkommande kontroller internt för att säkerställa upprätthållandet av denna policy

14.2 PeopleAnalytics ska på begäran, kunna visa efterlevnad mot dessa säkerhetskrav och andra säkerhetskrav eller säkerhetsåtgärder som avtalats med Kund.