

## **OFTTE STILLEDE SPØRGSMÅL OM DATABESKYTTELSE**

Dette dokument er beregnet til at besvare de mest almindelige spørgsmål, som vores kunder stiller om hvorfor og hvordan vi behandler personlige data.

### **1. Hvem er Insights?**

Vi er en global learning and development virksomhed med hovedkvarter i Storbritannien. Insights Learning & Development Limited ("ILD") er den primære ordregiver. ILD er registreret hos den engelske databeskyttelsesmyndighed, Information Commissioners Office ("ICO") under nummer Z7145849.

ILD har i mange år udviklet psykometriske værktøjer til at hjælpe mennesker med at forstå sig selv, andre og få mest muligt ud af de relationer, der påvirker dem på arbejdspladsen. Kerneydelsen er en unik personlig profil ("Profilen"), der kan bruges som udgangspunkt for en række videreuddannelser fra individuel coaching til teameffektivitet. Vores ydelser bruges i hele verden til personale- og organisationsudvikling.

ILD uddanner og akkrediterer Insights Discovery Practitioners. Disse er selvstændige undervisere, konsulenter eller medarbejdere i en virksomhed. Som akkrediteret Insights Discovery Practitioner har man adgang til vores online platform, hvor man kan oprette og administrere profiler.

For mere information om os [www.insights.com](http://www.insights.com).

### **2. Hvilke data har vi brug for?**

Insights Discovery-metoden bruger en enkel og mindeværdig model med fire farver til at hjælpe folk med at forstå deres personlige stil, deres styrker og den værdi, de tilføjer teamet. Vi kalder det farveenergiene. Det er den unikke blanding af ildrød, solgul, skovgrøn og havblå energier, som bestemmer, hvordan og hvorfor folk opfører sig, som de gør.

Til oprettelse af en profil indsamler Insights begrænsede personoplysninger om personen, såsom navn og e-mailadresse.

Typisk sender en Insights Accredited Practitioner et invitationslink til vores online evaluator med et spørgeskema til profilmodtagerne, der skal deltage i en workshop eller tilbagemelding. Profilens modtagere bekræfter, at de accepterer vores privatlivspolitik, og derefter angive deres navn, køn, virksomhedens e-mailadresse og referencekode for at udfylde evaluatorspørgeskemaet. Når profilen er færdig, leveres den til profilmodtageren og er tilgængelig på den Insights-onlinekonto. Profiler lagres, så den

Akkrediteret Practitioner kan forklare profilen mere detaljeret for profilmodtager. Profiler indeholder data, der er relevante for den enkelte profilmodtager. Men den eneste identificerende oplysninger, der er indeholdt i profilen, er modtagerens navn.

### 3. Er vi en controller eller en processor?

Vi er en uafhængig dataansvarlig og ikke en databehandler.

Akkrediteret Practitioner eller konsulenter, der arbejder på vores vegne for at levere workshops, indsamler data direkte fra den enkelte profilmodtager. Personprofilen leveres direkte til profilmodtageren. Der indsamles ingen data fra arbejdsgiveren, og profilen deles ikke rutinemæssigt med arbejdsgivere af os. Profilmottagere skal acceptere vores privatlivspolitik, før de udfylder vores evaluatorspørgeskema. Denne privatlivspolitik siger udtrykkeligt, at vi ikke vil dele profiler med andre end den relevante profilmottager og den akkrediteret Practitioner, der udfører opgaven. Vores profiler er til gavn for den enkelte profilmottager, der udfylder evalueringsspørgeskemaet. De udfyldes ikke på vegne af arbejdsgivere.

Det er udelukkende os, der bestemmer, hvilke personoplysninger der skal indsamles. Arbejdsgivere indsamler ikke personoplysninger direkte fra deres medarbejdere og giver dem til os. I stedet kommer medarbejderne direkte til os med disse data. Profilmottagerne kan derefter få adgang til deres profiler uafhængigt af hinanden på vores online platform. Det er derefter op til disse profilmottagerer at beslutte, hvad de vælger at gøre med deres profiler.

Derudover:

- Beslutter vi de gældende opbevaringsperioder for de personlige data i profilen. Vi handler ikke efter instrukser fra arbejdsgivere i forhold til disse data.
- Bestemmer vi indholdet af vores privatlivspolitik, der udstedes til profilmottagerne. Vi tager ikke imod instruktioner om indholdet af vores privatlivspolitik fra arbejdsgivere;
- Vi informerer enkeltpersoner om deres rettigheder i henhold til databeskyttelsesloven og handler efter deres anvisninger vedrørende disse data i modsætning til arbejdsgiveren; og
- Vi træffer uafhængige beslutninger vedrørende profilens data. For eksempel bestemmer vi, hvor data skal gemmes, og hvilke sikkerhedsforanstaltninger der skal gælde for disse data. Vi tager ikke imod instruktioner fra arbejdsgivere om disse spørgsmål.

Vi anerkender, at arbejdsgivere lejlighedsvis kan give os oplysninger om modtagerer (såsom e-mailadresser). Derfor mener vi fortsat, at vi er dataansvarlige i denne situation. Deling af data ændrer ikke på det faktum, at vi udøver den overordnede kontrol over formålet med og midler til behandling af personoplysninger i disse situationer. Databehandler har ikke de samme forpligtelser i henhold til databeskyttelseslovgivningen som dataansvarlige, og vi mener ikke, at det er passende for os at indtage denne rolle i betragtning af ovenstående oplysninger.

#### 4. Overholder vi lovgivningen om databeskyttelse?

Vi er en international gruppe af virksomheder. Vi overholder alle gældende regler for databeskyttelse love, hvor vi har selskaber. Vi har etableret vores globale juridiske ramme i overensstemmelse med General Data Protection Regulation (GDPR) (forordning (EU) 2916/679) ("EU GDPR"), UK GDPR (som bibeholdt i EU (Withdrawal Act) 2018 og Data Protection Act 2018 (DPA 2018)). Bestemmelserne i den britiske GDPR anvendes i overensstemmelse med den verdensomspændende dataforordning. Beskyttelsesregler, der giver os mulighed for at sikre, at data beskyttes i overensstemmelse med gældende love i hver jurisdiktion, vi opererer i.

Hvor det er muligt, er vi afhængige af tilstrækkelighed for dataoverførsler globalt. Det betyder, at de data under overførslen eller ved modtagerens modtagelse af personoplysningerne ikke være underlagt en beskyttelsesstandard, der er lavere end den standard, de får i henhold til Storbritanniens (eller den gældende jurisdiktions) databeskyttelseslove. Vi er i øjeblikket styret af Europa-Kommissionens beslutninger om tilstrækkeligheden af beskyttelsesniveauet, som er blevet vedtaget af Storbritannien efter udtrædelsen af EU.

For enhver overførsel af personlige data udenfor Storbritannien/EØS implementerer vi EU-standardens Kontraktbestemmelser ("EU SCCs") som indført af Europa-Kommissionen. For personlige dataoverførsler, der vedrører registrerede i Storbritannien, er det britiske tillæg (som udarbejdet af ICO) knyttet til EU's standardkontraktbestemmelser. Vi kræver, at enhver organisation, vi involverer i en dataoverførsel, har passende tekniske og sikkerhedsmæssige foranstaltninger på plads for at sikre, at data er tilstrækkeligt beskyttet. I overensstemmelse med GDPR-reglerne er vi, som den dataansvarlige, der overfører personoplysningerne, dataeksportøren.

Vi følger udviklingen i den britiske databeskyttelseslovgivning nøje og vil foretage de nødvendige ændringer i vores databeskyttelsesprocesser i forbindelse med lovgivningsmæssige ændringer. Vi vil kommunikere alle væsentlige ændringer, vi foretager med vores kunder og registrerede inden for 30 dage.

#### 5. Hvor opbevarer vi personlige data?

Alle personlige data, der indsamles gennem vores online evaluator spørgeskema, opbevares online i vores webapplikation. Insights Online-data hostes af Amazon Web Services (AWS) i et ISO 27001-certificeret datacenter i Storbritannien. Data fra den nye kundeplatform hostes af Amazon Web Services (AWS) i et ISO 27001-certificeret datacenter i EU. Personlige data, der indsamles på andre måder, herunder kontaktoplysninger på vores kunder, personlige data vedrørende akkreditering eller workshops, der udføres af os, opbevares i IT-tjenester, der administreres af os.

## 6. Hvilke teknisk-organisatoriske tiltag har vi implementeret?

Vi anvender en række tekniske og sikkerhedsmæssige foranstaltninger for at sikre overholdelse af datalovgivningen, beskyttelseslove og beskyttelse af personlige data.

Vi er afhængige af certificerede datacentre til sikker datalagring og -behandling og kræver kryptering, hvor det er muligt. For mere information om AWS' sikkerhedsforanstaltninger, besøg [ISO/IEC 27001:2022 Compliance - Amazon Web Services \(AWS\)](#).

Vores informationssikkerhedsstyringssystem er i øjeblikket baseret på ISO 27001 og følger anbefalinger fra NIST Cybersecurity Framework. Fra maj 2024 opnåede vi ISO 27001:2022 akkreditering i november 2023. Denne akkreditering kræver et sæt standarder for systemer for at sikre, at alle lovgivningsmæssige og regulatoriske krav overholdes. Denne certificering illustrerer den forpligtelse, vi har til sikkerheden af data og systemer til at understøtte datahåndtering.

Vi sikrer også, at:

- En disaster recovery-plan er i drift med mål for gendannelsestid og med planlagte årlige tests.
- Penetrationstest udføres regelmæssigt på alle systemer for at sikre overholdelse.
- Alle tredjepartsudbydere er kontrolleret for overholdelse af CREST-certificering.
- Dataovervågning er konstant i drift under lagring for at sikre dataintegritet.
- Data bortskaffes sikkert, og sikkerhedslogfiler opbevares i en periode på 180 dage (i praksis ca. 6 måneder).

## 7. Hvem overfører vi personlige data til?

Vi deler personlige data som angivet i vores privatlivspolitik. For eksempel deler vi profiler med profilmodtagere og den akkrediteret Practitioner.

Vi deler teamhjul eller aggregerede rapporter (men aldrig profiler) med den organisation, der har bestilt workshoppen eller den individuelle debriefing med henblik på at styrke samarbejdet gennem teameffektivitet.

Vi bruger ikke data til andre formål end dem, der er beskrevet i privatlivspolitikken, og vi sælger ikke oplysninger til tredjeparter.

Vi anvender typisk ikke databehandlere, men kan lejlighedsvis anvende tredjepartsprintere til udskrivning af profiler, hvor det er nødvendigt. Alle tredjeparter, vi anvender som databehandlere, er forpligtet til at overholde gældende databeskyttelseslove. De skal også overbevise os om, at de har implementeret passende sikkerhedsforanstaltninger for at sikre, at alle personlige oplysninger er beskyttet.

## **8. Hvordan kan profilmodtagere udøve deres rettigheder?**

Profilmodtagere skal kontakte os på [dpo@insights.com](mailto:dpo@insights.com) for at udøve deres rettigheder under gældende databeskyttelseslove.

## **9. Hvem er ansvarlig for informationssikkerheden hos Insights?**

Vores sikkerhedschef er ansvarlig for sikkerheden af alle data her og kan kontaktes på: [security@insights.com](mailto:security@insights.com)

## **10. Har Insights udpeget en databeskyttelsesansvarlig?**

Ja, det gør vi. Vores DPO er baseret på vores hovedkontor i Storbritannien og kan kontaktes på: [dpo@insights.com](mailto:dpo@insights.com).