

Databehandleraftale – Trackrs

Version 1.1 · gælder fra 1. december 2026

PARTER

Standardkontraktsbestemmelser i henhold til artikel 28, stk. 3, i forordning 2016/679 (databeskyttelsesforordningen) med henblik på databehandlerens behandling af personoplysninger

Version 1.1 · Gældende fra 1. december 2026

mellem

[virksomhedens navn] · CVR [CVR-nr.] · [adresse]

herefter "den dataansvarlige"

og

Rasmussen Solutions ApS · CVR 42296244 · Skovvej 12, 4622 Havdrup

herefter "databehandleren"

der hver især er en "part" og sammen udgør "parterne"

HAR AFTALT følgende standardkontraktsbestemmelser (Bestemmelserne) med henblik på at overholde databeskyttelsesforordningen og sikre beskyttelse af privatlivets fred og fysiske personers grundlæggende rettigheder og frihedsrettigheder

Aftalen er indgået elektronisk ved accept i Trackrs. Se kvitteringen for accept i bestemmelse 14.5 og Bilag D.1.

2. PRÆAMBEL

2.1. Disse Bestemmelser fastsætter databehandlerens rettigheder og forpligtelser, når denne foretager behandling af personoplysninger på vegne af den dataansvarlige.

2.2. Disse bestemmelser er udformet med henblik på parternes efterlevelse af artikel 28, stk. 3, i Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (databeskyttelsesforordningen).

2.3. I forbindelse med leveringen af Trackrs, en platform til registrering og sporing af værktøj og udstyr (RFID, BLE og QR), udlån, service og tilstedeværelse på lokationer (web på app.trackrs.dk og apps til iOS og Android) behandler databehandleren personoplysninger på vegne af den dataansvarlige i overensstemmelse med disse Bestemmelser.

2.4. Bestemmelserne har forrang i forhold til eventuelle tilsvarende bestemmelser i andre aftaler mellem parterne.

2.5. Der hører fire bilag til disse Bestemmelser, og bilagene udgør en integreret del af Bestemmelserne.

2.6. Bilag A indeholder nærmere oplysninger om behandlingen af personoplysninger, herunder om behandlingens formål og karakter, typen af personoplysninger, kategorierne af registrerede og varighed af behandlingen.

2.7. Bilag B indeholder den dataansvarliges betingelser for databehandlerens brug af underdatabehandlere og en liste af underdatabehandlere, som den dataansvarlige har godkendt brugen af.

2.8. Bilag C indeholder den dataansvarliges instruks for så vidt angår databehandlerens behandling af personoplysninger, en beskrivelse af de sikkerhedsforanstaltninger, som databehandleren som minimum skal gennemføre, og hvordan der føres tilsyn med databehandleren og eventuelle underdatabehandlere.

2.9. Bilag D indeholder bestemmelser vedrørende andre aktiviteter, som ikke af omfattet af Bestemmelserne.

2.10. Bestemmelserne med tilhørende bilag skal opbevares skriftligt, herunder elektronisk, af begge parter.

2.11. Disse Bestemmelser frigør ikke databehandleren fra forpligtelser, som databehandleren er pålagt efter databeskyttelsesforordningen eller enhver anden lovgivning.

3. DEN DATAANSVARLIGES RETTIGHEDER OG FORPLIGTELSE

3.1. Den dataansvarlige er ansvarlig for at sikre, at behandlingen af personoplysninger sker i overensstemmelse med databeskyttelsesforordningen (se forordningens artikel 24), databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser.

3.2. Den dataansvarlige har ret og pligt til at træffe beslutninger om, til hvilke(t) formål og med hvilke hjælpemidler, der må ske behandling af personoplysninger.

3.3. Den dataansvarlige er ansvarlig for, blandt andet, at sikre, at der er et behandlingsgrundlag for behandlingen af personoplysninger, som databehandleren instrueres i at foretage.

4. DATABEHANDLEREN HANDLER EFTER INSTRUKS

4.1. Databehandleren må kun behandle personoplysninger efter dokumenteret instruks fra den dataansvarlige, medmindre det kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som databehandleren er underlagt. Denne instruks skal være specificeret i bilag A og C. Efterfølgende instruks kan også gives af den dataansvarlige, mens der sker behandling af personoplysninger, men instruksen skal altid være dokumenteret og opbevares skriftligt, herunder elektronisk, sammen med disse Bestemmelser.

4.2. Databehandleren underretter omgående den dataansvarlige, hvis en instruks efter vedkommendes mening er i strid med denne forordning eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.

5. FORTROLIGHED

5.1. Databehandleren må kun give adgang til personoplysninger, som behandles på den dataansvarliges vegne, til personer, som er underlagt databehandlerens instruktionsbeføjelser, som har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt, og kun i det nødvendige omfang. Listen af personer, som har fået tildelt adgang, skal løbende gennemgås. På baggrund af denne gennemgang kan adgangen til personoplysninger lukkes, hvis adgangen ikke længere er nødvendig, og personoplysningerne skal herefter ikke længere være tilgængelige for disse personer.

5.2. Databehandleren skal efter anmodning fra den dataansvarlige kunne påvise, at de pågældende personer, som er underlagt databehandlerens instruktionsbeføjelser, er underlagt ovennævnte tavshedspligt.

6. BEHANDLINGSSIKKERHED

6.1. Databeskyttelsesforordningens artikel 32 fastslår, at den dataansvarlige og databehandleren, under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder, gennemfører passende tekniske og organisatoriske foranstaltninger for at sikre et beskyttelsesniveau, der passer til disse risici.

Den dataansvarlige skal vurdere risiciene for fysiske personers rettigheder og frihedsrettigheder som behandlingen udgør og gennemføre foranstaltninger for at imødegå disse risici. Afhængig af deres relevans kan det omfatte:

- a. Pseudonymisering og kryptering af personoplysninger
- b. evne til at sikre vedvarende fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og -tjenester
- c. evne til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk

hændelse

d. en procedure for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerhed.

6.2. Efter forordningens artikel 32 skal databehandleren – uafhængigt af den dataansvarlige – også vurdere risiciene for fysiske personers rettigheder som behandlingen udgør og gennemføre foranstaltninger for at imødegå disse risici. Med henblik på denne vurdering skal den dataansvarlige stille den nødvendige information til rådighed for databehandleren som gør vedkommende i stand til at identificere og vurdere sådanne risici.

6.3. Derudover skal databehandleren bistå den dataansvarlige med vedkommendes overholdelse af den dataansvarliges forpligtelse efter forordningens artikel 32, ved bl.a. at stille den nødvendige information til rådighed for den dataansvarlige vedrørende de tekniske og organisatoriske sikkerhedsforanstaltninger, som databehandleren allerede har gennemført i henhold til forordningens artikel 32, og al anden information, der er nødvendig for den dataansvarliges overholdelse af sin forpligtelse efter forordningens artikel 32.

Hvis imødegåelse af de identificerede risici – efter den dataansvarliges vurdering – kræver gennemførelse af yderligere foranstaltninger end de foranstaltninger, som databehandleren allerede har gennemført, skal den dataansvarlige angive de yderligere foranstaltninger, der skal gennemføres, i bilag C.

7. ANVENDELSE AF UNDERDATABEHANDLERE

7.1. Databehandleren skal opfylde de betingelser, der er omhandlet i databeskyttelsesforordningens artikel 28, stk. 2, og stk. 4, for at gøre brug af en anden databehandler (en underdatabehandler).

7.2. Databehandleren må således ikke gøre brug af en underdatabehandler til opfyldelse af disse Bestemmelser uden forudgående generel skriftlig godkendelse fra den dataansvarlige.

7.3. Databehandleren har den dataansvarliges generelle godkendelse til brug af underdatabehandlere. Databehandleren skal skriftligt underrette den dataansvarlige om eventuelle planlagte ændringer vedrørende tilføjelse eller udskiftning af underdatabehandlere med mindst 30 dages varsel og derved give den dataansvarlige mulighed for at gøre indsigelse mod sådanne ændringer inden brugen af de(n) omhandlede underdatabehandler(e). Længere varsel for underretning i forbindelse med specifikke behandlingsaktiviteter kan angives i bilag B. Listen over underdatabehandlere, som den dataansvarlige allerede har godkendt, fremgår af bilag B.

7.4. Når databehandleren gør brug af en underdatabehandler i forbindelse med udførelse af specifikke behandlingsaktiviteter på vegne af den dataansvarlige, skal databehandleren, gennem en kontrakt eller andet retligt dokument i henhold til EU-retten eller medlemsstaternes nationale ret, pålægge underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der fremgår af disse Bestemmelser, hvorved der navnlig stilles de fornødne garantier for, at underdatabehandleren vil gennemføre de tekniske og organisatoriske foranstaltninger på en sådan måde, at behandlingen overholder kravene i disse Bestemmelser og databeskyttelsesforordningen.

Databehandleren er derfor ansvarlig for at kræve, at underdatabehandleren som minimum overholder databehandlerens forpligtelser efter disse Bestemmelser og databeskyttelsesforordningen.

7.5. Underdatabehandleraftale(r) og eventuelle senere ændringer hertil sendes – efter den dataansvarliges anmodning herom – i kopi til den dataansvarlige, som herigennem har mulighed for at sikre sig, at tilsvarende databeskyttelsesforpligtelser som følger af disse Bestemmelser er pålagt underdatabehandleren. Bestemmelser om kommercielle vilkår, som ikke påvirker det databeskyttelsesretlige indhold af underdatabehandleraftalen, skal ikke sendes til den dataansvarlige.

7.6. (Valgfri bestemmelse – ikke valgt.)

7.7. Hvis underdatabehandleren ikke opfylder sine databeskyttelsesforpligtelser, forbliver databehandleren fuldt ansvarlig over for den dataansvarlige for opfyldelsen af underdatabehandlerens forpligtelser. Dette påvirker ikke de registreredes rettigheder, der følger af databeskyttelsesforordningen, herunder særligt forordningens artikel 79 og 82, over for den dataansvarlige og databehandleren, herunder underdatabehandleren.

8. OVERFØRSEL TIL TREDJELANDE ELLER INTERNATIONALE ORGANISATIONER

8.1. Enhver overførsel af personoplysninger til tredjelande eller internationale organisationer må kun foretages af databehandleren på baggrund af dokumenteret instruks herom fra den dataansvarlige og skal altid ske i overensstemmelse med databeskyttelsesforordningens kapitel V.

8.2. Hvis overførsel af personoplysninger til tredjelande eller internationale organisationer, som databehandleren ikke er blevet instrueret i at foretage af den dataansvarlige, kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som databehandleren er underlagt, skal databehandleren underrette den dataansvarlige om dette retlige krav inden behandling, medmindre den pågældende ret forbyder en sådan underretning af hensyn til vigtige samfundsmæssige interesser.

8.3. Uden dokumenteret instruks fra den dataansvarlige kan databehandleren således ikke inden for rammerne af disse Bestemmelser:

- a. overføre personoplysninger til en dataansvarlig eller databehandler i et tredjeland eller en international organisation
- b. overlade behandling af personoplysninger til en underdatabehandler i et tredjeland
- c. behandle personoplysningerne i et tredjeland

8.4. Den dataansvarliges instruks vedrørende overførsel af personoplysninger til et tredjeland, herunder det eventuelle overførselsgrundlag i databeskyttelsesforordningens kapitel V, som overførslen er baseret på, skal angives i bilag C.6.

8.5. Disse Bestemmelser skal ikke forveksles med standardkontraktsbestemmelser som omhandlet i databeskyttelsesforordningens artikel 46, stk. 2, litra c og d, og disse Bestemmelser kan ikke udgøre et grundlag for overførsel af personoplysninger som omhandlet i databeskyttelsesforordningens kapitel V.

9. BISTAND TIL DEN DATAANSVARLIGE

9.1. Databehandleren bistår, under hensyntagen til behandlingens karakter, så vidt muligt den dataansvarlige ved hjælp af passende tekniske og organisatoriske foranstaltninger med opfyldelse af den dataansvarliges forpligtelse til at besvare anmodninger om udøvelsen af de registreredes rettigheder som fastlagt i databeskyttelsesforordningens kapitel III.

Dette indebærer, at databehandleren så vidt muligt skal bistå den dataansvarlige i forbindelse med, at den dataansvarlige skal sikre overholdelsen af:

- a. oplysningspligten ved indsamling af personoplysninger hos den registrerede
- b. oplysningspligten, hvis personoplysninger ikke er indsamlet hos den registrerede
- c. indsigtsheden
- d. retten til berigtigelse
- e. retten til sletning ("retten til at blive glemt")
- f. retten til begrænsning af behandling
- g. underretningspligten i forbindelse med berigtigelse eller sletning af personoplysninger eller begrænsning af behandling
- h. retten til dataportabilitet
- i. retten til indsigelse
- j. retten til ikke at være genstand for en afgørelse, der alene er baseret på automatisk behandling, herunder profilering

9.2. I tillæg til databehandlerens forpligtelse til at bistå den dataansvarlige i henhold til Bestemmelse 6.3., bistår databehandleren endvidere, under hensyntagen til behandlingens karakter og de oplysninger, der er tilgængelige for databehandleren, den dataansvarlige med:

- a. den dataansvarliges forpligtelse til uden unødigt forsinkelse og om muligt senest 72 timer, efter at denne er blevet bekendt med det, at anmelde brud på persondatasikkerheden til den kompetente tilsynsmyndighed, Datatilsynet, medmindre at det er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder
 - b. den dataansvarliges forpligtelse til uden unødigt forsinkelse at underrette den registrerede om brud på persondatasikkerheden, når bruddet sandsynligvis vil medføre en høj risiko for fysiske personers rettigheder og frihedsrettigheder
 - c. den dataansvarliges forpligtelse til forud for behandlingen at foretage en analyse af de påtænkte behandlingsaktiviteters konsekvenser for beskyttelse af personoplysninger (en konsekvensanalyse)
 - d. den dataansvarliges forpligtelse til at høre den kompetente tilsynsmyndighed, Datatilsynet, inden behandling, såfremt en konsekvensanalyse vedrørende databeskyttelse viser, at behandlingen vil føre til høj risiko i mangel af foranstaltninger truffet af den dataansvarlige for at begrænse risikoen.
- 9.3. Parterne skal i bilag C angive de fornødne tekniske og organisatoriske foranstaltninger, hvormed databehandleren skal bistå den dataansvarlige samt i hvilket omfang og udstrækning. Det gælder for de forpligtelser, der følger af Bestemmelse 9.1. og 9.2.

10. UNDERRETNING OM BRUD PÅ PERSONDATASIKKERHEDEN

- 10.1. Databehandleren underretter uden unødigt forsinkelse den dataansvarlige efter at være blevet opmærksom på, at der er sket et brud på persondatasikkerheden.
- 10.2. Databehandlerens underretning til den dataansvarlige skal om muligt ske senest 24 timer efter, at denne er blevet bekendt med bruddet, sådan at den dataansvarlige kan overholde sin forpligtelse til at anmelde bruddet på persondatasikkerheden til den kompetente tilsynsmyndighed, jf. databeskyttelsesforordningens artikel 33.
- 10.3. I overensstemmelse med Bestemmelse 9.2.a skal databehandleren bistå den dataansvarlige med at foretage anmeldelse af bruddet til den kompetente tilsynsmyndighed. Det betyder, at databehandleren skal bistå med at tilvejebringe nedenstående information, som ifølge artikel 33, stk. 3, skal fremgå af den dataansvarliges anmeldelse af bruddet til den kompetente tilsynsmyndighed:
 - a. karakteren af bruddet på persondatasikkerheden, herunder, hvis det er muligt, kategorierne og det omtrentlige antal berørte registrerede samt kategorierne og det omtrentlige antal berørte registreringer af personoplysninger
 - b. de sandsynlige konsekvenser af bruddet på persondatasikkerheden
 - c. de foranstaltninger, som den dataansvarlige har truffet eller foreslår truffet for at håndtere bruddet på persondatasikkerheden, herunder, hvis det er relevant, foranstaltninger for at begrænse dets mulige skadevirkninger.
- 10.4. Parterne skal i bilag C angive den information, som databehandleren skal tilvejebringe i forbindelse med sin bistand til den dataansvarlige i dennes forpligtelse til at anmelde brud på persondatasikkerheden til den kompetente tilsynsmyndighed.

11. SLETNING OG RETURNERING AF OPLYSNINGER

- 11.1. Ved ophør af tjenesterne vedrørende behandling af personoplysninger, er databehandleren forpligtet til at slette alle personoplysninger, der er blevet behandlet på vegne af den dataansvarlige og bekræfte over for den dataansvarlige, at oplysningerne er slettet, medmindre EU-retten eller medlemsstaternes nationale ret foreskriver opbevaring af personoplysningerne.

12. REVISION, HERUNDER INSPEKTION

- 12.1. Databehandleren stiller alle oplysninger, der er nødvendige for at påvise overholdelsen af

databeskyttelsesforordningens artikel 28 og disse Bestemmelser, til rådighed for den dataansvarlige og giver mulighed for og bidrager til revisioner, herunder inspektioner, der foretages af den dataansvarlige eller en anden revisor, som er bemyndiget af den dataansvarlige.

12.2. Procedurene for den dataansvarliges revisioner, herunder inspektioner, med databehandleren og underdatabehandlere er nærmere angivet i Bilag C.7. og C.8.

12.3. Databehandleren er forpligtet til at give tilsynsmyndigheder, som efter gældende lovgivningen har adgang til den dataansvarliges eller databehandlerens faciliteter, eller repræsentanter, der optræder på tilsynsmyndighedens vegne, adgang til databehandlerens fysiske faciliteter mod behørig legitimation.

13. PARTERNES AFTALE OM ANDRE FORHOLD

13.1. Parterne kan aftale andre bestemmelser vedrørende tjenesten vedrørende behandling af personoplysninger om f.eks. erstatningsansvar, så længe disse andre bestemmelser ikke direkte eller indirekte strider imod Bestemmelserne eller forringer den registreredes grundlæggende rettigheder og frihedsrettigheder, som følger af databeskyttelsesforordningen.

14. IKRAFTTRÆDEN OG OPHØR

14.1. Bestemmelserne træder i kraft på datoen for begge parters underskrift heraf.

14.2. Begge parter kan kræve Bestemmelserne genforhandlet, hvis lovændringer eller uhensigtsmæssigheder i Bestemmelserne giver anledning hertil.

14.3. Bestemmelserne er gældende, så længe tjenesten vedrørende behandling af personoplysninger varer. I denne periode kan Bestemmelserne ikke opsiges, medmindre andre bestemmelser, der regulerer levering af tjenesten vedrørende behandling af personoplysninger, aftales mellem parterne.

14.4. Hvis levering af tjenesterne vedrørende behandling af personoplysninger ophører, og personoplysningerne er slettet eller returneret til den dataansvarlige i overensstemmelse med Bestemmelse 11.1 og Bilag C.4, kan Bestemmelserne opsiges med skriftlig varsel af begge parter.

14.5. Underskrift

Bestemmelserne er underskrevet elektronisk af begge parter som beskrevet i Bilag D.1.

Registreringen af accepten (aftaleversion, kontrolsum af den accepterede tekst, tidspunkt i UTC, brugerens navn og e-mail, oplyst IP-adresse og browser) udgør den dataansvarliges underskrift, jf. Bilag D.1.

PÅ VEGNE AF DATABEHANDLEREN

Virksomhed	Rasmussen Solutions ApS, CVR 42296244
Udstedt	Aftaleversion 1.1 offentliggjort 19. oktober 2026, gælder fra 1. december 2026 og stillet til accept i Trackrs

15. KONTAKTPERSONER HOS DEN DATAANSVARLIGE OG DATABEHANDLEREN

15.1. Parterne kan kontakte hinanden via nedenstående kontaktpersoner.

15.2. Parterne er forpligtet til løbende at orientere hinanden om ændringer vedrørende kontaktpersoner.

Den dataansvarliges kontaktperson er som udgangspunkt brugeren, der accepterede aftalen. Navn og e-mail fremgår af registreringen af accepten. Ændring af kontaktperson sker ved e-mail til privacy@trackrs.dk, jf. Bilag D.2.3.

DATABASEHANDLEREN

Virksomhed

Rasmussen Solutions ApS

E-mail

privacy@trackrs.dk

BILAG A – OPLYSNINGER OM BEHANDLINGEN

A.1. Formålet med databehandlerens behandling af personoplysninger på vegne af den dataansvarlige

Databehandleren behandler personoplysninger for at levere Trackrs til den dataansvarlige. Trackrs bruges til at:

- registrere den dataansvarliges værktøj og udstyr og vise, hvor det er, og hvem der har det
- registrere udlån af værktøj til navngivne medarbejdere og flytninger mellem lokationer, sager og køretøjer
- registrere, når medarbejdere og værktøj kommer til og forlader en lokation (tilstedeværelse), ud fra telefonens position, BLE-signaler, RFID-læsere og netværk
- håndtere savnet og stjålet værktøj, herunder anmeldelser til politi og forsikring
- planlægge og dokumentere service og eftersyn
- styre sager, brugere, roller og afdelinger
- sende notifikationer og alarmer (push og e-mail)
- give support og modtage feedback, også via Trackrs' MCP-server og AI-briller
- drive og fejlfrette tjenesten

A.2. Karakteren af behandlingen

Opbevaring, strukturering, visning, søgning, ændring og eksport af data, som den dataansvarliges brugere indtaster. Dertil kommer data, som enheder og apps indsamler automatisk:

- Position fra medarbejderes telefoner: appen beder om lokationstilladelse, på iOS også "Altid". Den bruger telefonens GPS til at afgøre, om medarbejderen er på eller ved en af den dataansvarliges lokationer. Den aktuelle tilstedeværelse gemmes med GPS-koordinater. Hændelser for ankomst og afgang gemmes som historik.
- Observationer: når appen eller en læser ser en BLE-tag, et værktøj eller et netværk, gemmes en observation med tidspunkt, bruger og GPS-position.
- Scanninger fra faste RFID-læsere: sendes via MQTT (Stackhero) og gemmes i tidsseriedatabaser (InfluxDB Cloud og PostgreSQL/Timescale). Scanningerne indeholder læserens id (IMEI/IMSI), tag-id (EPC) og signalstyrke, ikke medarbejderes identitet.
- Opslag: adresser (Dataforsyningen), nummerplader (nummerplade.net), virksomheder (cvrapi.dk). Der sendes kun søgeteksten.
- Kortvisning og adresseopslag: Google Maps Platform i web og app (se Bilag B).
- AI: billeder fra Trackrs' AI-briller og tale fra appen behandles af Anthropic og OpenAI for at oprette og finde værktøj. Indkommen feedback og supportsager analyseres af Anthropic.
- Afsendelse: e-mail (Mailgun) og push (Expo, Google, Apple). Udlånserklæringer og alarmer behandles i Firebase.
- Logning: aktivitetslog og bevægelseshistorik (hvem flyttede hvad).

A.3. Typer af personoplysninger

Medarbejdere og brugere hos den dataansvarlige

- Navn, e-mail, rolle, afdeling, profilbillede eller initialer, seneste aktivitet, push-tokens, loginoplysninger fra RsConnect
- Positionsdata: GPS-koordinater fra telefonen i forbindelse med tilstedeværelse og observationer. Tidspunkter for ankomst til og afgang fra lokationer. Historik over BLE-, værktøjs-, netværks- og prioritetsobservationer knyttet til brugeren.

- Udlån (hvilket værktøj, hvornår, til hvem), bevægelseshistorik (hvem flyttede værktøjet), aktivitetslog
- Billeder og tale fra AI-brillerne og appen, når medarbejderen bruger dem
- Supporthenvendelser og feedback

Tredjeparter

- Anmeldelser af savnet værktøj: lokation, værktøj med serienummer og foto, sidst set, journalnummer hos politiet, skadenummer hos forsikringen, anslået værdi og en fritekstnote (kan indeholde oplysninger om personer)
- Kontaktpersoner hos kunder og på sager, nummerplader på køretøjer

Følsomme oplysninger (artikel 9) og strafbare forhold (artikel 10)

Trackrs har ingen felter til artikel 9- eller artikel 10-oplysninger. Anmeldelsens fritekstnote kan dog indeholde oplysninger om mistanke om strafbare forhold, hvis den dataansvarliges brugere skriver dem.

A.4. Kategorier af registrerede

- Den dataansvarliges medarbejdere og øvrige brugere
- Personer, der optræder i anmeldelser, på fotos eller som kontaktpersoner på sager

A.5. Behandlingens varighed

Behandlingen kan begynde, når Bestemmelserne træder i kraft. Den varer, så længe den dataansvarlige har en aktiv virksomhedskonto i Trackrs, og derefter indtil oplysningerne er slettet efter Bilag C.4.

BILAG B – UNDERDATABEHANDLERE

B.1. Godkendte underdatabehandlere

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af følgende underdatabehandlere

DPF = EU-US Data Privacy Framework (afgørelse (EU) 2023/1795). SCC = Kommissionens standardkontraktbestemmelser (afgørelse (EU) 2021/914).

NAVN	CVR/REG.-NR.	ADRESSE	BESKRIVELSE AF BEHANDLING	PLACERING	OVERFØRSELSSGRUNDLAG
Microsoft Ireland Operations Ltd. (Microsoft Azure)	–	One Microsoft Place, Leopardstown, Dublin 18, Irland	API (App Service), PostgreSQL-databaser, fillagring (Blob), Key Vault	EU – North Europe (Irland)	Data opbevares i EU. Eventuel support- og drifts adgang fra tredjelande: SCC i Microsofts Products and Services Data Protection Addendum
InfluxData Inc. (InfluxDB Cloud Serverless)	–	San Francisco, USA	Tidsserier med RFID-scanninger (læser-id, tag-id, signalstyrke)	EU – AWS Frankfurt (eu-central-1)	Data opbevares i EU. Eventuel adgang fra USA: DPF og SCC i InfluxDatas DPA
Stackhero (MQTT-mægler)	RCS Paris 512 366 378	Paris, Frankrig	Formidling af scanninger fra RFID-læsere	EU	EU-selskab. Ingen overførsel fra databehandleren

Google Cloud EMEA Ltd. (Firebase)	–	Dublin, Irland	Udlånserklæringer, alarmer via Pub/Sub, Cloud Functions	EU – Functions europe-west3 (Frankfurt) og Firestore i EU	Data opbevares i EU. Eventuel adgang fra USA: DPF (Google LLC) og SCC i Googles Cloud Data Processing Addendum
Google Cloud EMEA Ltd. (Firebase Cloud Messaging)	–	Dublin, Irland	Push-notifikationer til Android-enheder (push-token og beskedtekst)	Globalt, herunder USA	DPF (Google LLC) og SCC i Firebase Data Processing and Security Terms
650 Industries, Inc. (Expo)	–	Californien, USA	Push-notifikationer til appen (videresendes til Google og Apple)	USA	DPF og SCC (modul 2) i Expos vilkår
Mailgun Technologies, Inc. (Sinch)	–	Texas, USA	E-mail	EU – Mailguns EU-region	Indhold behandles i EU. Konto- og afsendelsesdata kan tilgås fra USA: DPF og SCC i Sinch' DPA
Anthropic Ireland, Limited	–	Irland	AI-briller (billeder og tekst) og analyse af feedback og supportsager. Input og output slettes hos Anthropic inden for 30 dage og bruges ikke til træning	USA	SCC (modul 2/3) i Anthropics Data Processing Addendum. Anthropic er ikke DPF-certificeret
OpenAI Ireland Ltd.	–	Dublin, Irland	Omsætning af tale til tekst for AI-brillerne og appen	USA	SCC i OpenAIs Data Processing Addendum. OpenAI er ikke DPF-certificeret
GitHub, Inc.	–	88 Colin P. Kelly Jr. St, San Francisco, CA, USA	Supportsager og feedback fra MCP	USA	DPF og SCC i GitHubs Data Protection Agreement
Raintank, Inc. (Grafana Labs, Grafana Cloud)	–	New York, USA	Overvågning og driftslogge	EU – Stockholm (eu-north-0)	Data opbevares i EU. Eventuel adgang fra USA: DPF og SCC (modul 2/3) i Grafana Labs' databehandleraftale
Netlify, Inc.	–	San Francisco, USA	Hosting af web (app.trackrs.dk). Netlify ser trafikken	Globalt CDN	DPF og SCC i Netlifs DPA

Den dataansvarliges egne forbindelser er ikke underdatabehandlere. Det gælder forbindelser til Mesterplan, MilePro og e-conomic, API-nøgler, som den dataansvarlige selv udsteder, og AI-assisterter (MCP-klienter), som den dataansvarlige selv forbinder.

Følgende er selvstændigt dataansvarlige eller opslagstjenester og heller ikke underdatabehandlere:

- Google Maps Platform (kort og adresseopslag) leveres på Googles vilkår for EØS, hvor Google er selvstændig dataansvarlig. Google modtager brugerens IP-adresse, kortudsnit og søgte adresser. Der sendes ingen øvrige data fra Trackrs.
- Apple (Apple Push Notification service) leverer push-beskeder til iOS-enheder. Apple tilbyder ingen databehandleraftale for tjenesten. Databehandleren sender kun push-token og en kort beskedtekst uden følsomme oplysninger.
- Dataforsyningen (Klimadatastyrelsen), nummerplade.net og cvrapi.dk er opslagstjenester, der kun modtager søgeteksten (adresse, nummerplade eller CVR-nummer).
- Stripe (abonnementsbetaling) behandler kun databehandlerens egne kundeoplysninger. Her er databehandleren dataansvarlig, og Stripe beskrives i privatlivspolitikken.

Databehandlerens egne systemer: RsConnect (login) og databehandlerens egen Grafana-installation. Cloudflare bruges kun til DNS og ser ingen indholdsdata.

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af ovennævnte underdatabehandlere for den beskrevne behandlingsaktivitet. Databehandleren må ikke – uden den dataansvarliges skriftlige godkendelse – gøre brug af en underdatabehandler til en anden behandlingsaktivitet end den beskrevne og aftalte eller gøre brug af en anden underdatabehandler til denne behandlingsaktivitet.

Den til enhver tid gældende liste offentliggøres på <https://trackrs.dk/da/gdpr.html> med en ændringslog (dato, ændring, begrundelse). Listen på siden udgør Bilag B.1 som ændret efter proceduren i B.2.

B.2. Varsel for godkendelse af underdatabehandlere

B.2.1. Underretning efter Bestemmelse 7.3 gives skriftligt på begge disse måder:

- a) e-mail fra databehandleren til den dataansvarliges kontaktperson efter Bestemmelse 15 og til alle brugere med administratorrolle i virksomheden, og
- b) en ny linje i ændringsloggen på <https://trackrs.dk/da/gdpr.html>.

Fristen på 30 dage regnes fra afsendelsen af e-mailen. Databehandleren registrerer for hver virksomhed, hvornår e-mailen er sendt.

B.2.2. Underretningen angiver underdatabehandlerens navn, adresse og registreringsnummer, behandlingsaktiviteten, kategorierne af personoplysninger, placering af behandlingen samt overførselsgrundlaget efter kapitel V, hvis behandlingen sker i et tredjeland.

B.2.3. Den dataansvarlige kan gøre indsigelse skriftligt til privacy@trackrs.dk inden for varslingsperioden. Indsigelsen bør begrundes i databeskyttelsesmæssige forhold. Databehandleren tager ikke den pågældende underdatabehandler i brug for den dataansvarliges personoplysninger, før indsigelsen er afklaret. Kan parterne ikke nå til enighed, kan den dataansvarlige opsiges hovedaftalen til ophør, inden ændringen træder i kraft, uden gebyr og med forholdsmæssig tilbagebetaling af forudbetalt abonnement for perioden efter ophøret.

B.2.4. Følgende behandlingsaktiviteter kræver længere varsel: ingen.

BILAG C – INSTRUKS VEDRØRENDE BEHANDLING AF PERSONOPLYSNINGER

C.1. Behandlingens genstand/instruks

Databehandleren driver Trackrs og udfører de behandlinger, der er beskrevet i Bilag A, når den dataansvarliges brugere bruger tjenestens funktioner. Den dataansvarliges konfiguration udgør dokumenteret instruks: oprettelse af lokationer,

aktivering af tilstedeværelse og BLE, roller og rettigheder, og hvilke integrationer der forbindes. Positionsdata om medarbejdere behandles kun for at bestemme tilstedeværelse ved den dataansvarliges lokationer og værktøjets placering, ikke for at følge medarbejdere i øvrigt. Se også Bilag D.6.

C.2. Behandlingssikkerhed

Sikkerhedsniveauet skal afspejle, at behandlingen omfatter systematisk registrering af medarbejderes position fra deres telefoner, også i baggrunden. Det giver høj risiko for de registreredes privatliv. Der skal derfor etableres et højt sikkerhedsniveau for adgangskontrol til positions- og tilstedeværelsesdata.

Databehandleren gennemfører som minimum:

- Kryptering: TLS mellem klienter og servere. Kryptering i hvile i Azure-database og fillagring. Hemmeligheder opbevares i Key Vault.
- Adskillelse og adgangskontrol: alle data afgrænses til virksomheds-id. Rettigheder styres af roller. Login sker via RsConnect. Alle brugere i virksomheden kan se, hvem der er registreret som til stede på en lokation.
- Genopretning: automatisk backup af PostgreSQL med 7 dages genopretning (uden geo-redundans). Fillagring har 30 dages blød sletning.
- Afprøvning og evaluering: afhængigheder og infrastruktur opdateres løbende. Ændringer gennemgås og deployes via CI/CD (GitHub Actions). Databehandleren gennemgår sikkerhedsforanstaltningerne mindst én gang om året og ved væsentlige ændringer.
- Adgang via internettet, transmission og opbevaring: kun efter login. RFID-læsere forbinder til MQTT-mægleren med adgangsoplysninger over en krypteret forbindelse.
- Fysisk sikring: datacentre hos underdatabehandlerne. Databehandleren har ingen egne servere med kundedata.
- Hjemme-/fjernarbejde: adgang til produktionssystemer er begrænset til databehandlerens egne udviklere, sker med personlige konti fra krypterede arbejdsstationer og lukkes, når den ikke længere er nødvendig.
- Logning: aktivitetslog over ændringer (hvem, hvad, hvornår) og bevægelseshistorik.

C.3. Bistand til den dataansvarlige

- Registreredes rettigheder: den dataansvarlige kan selv se og rette de fleste data. Sletning i tjenesten er blød sletning (data markeres som slettet). Anmodninger om at slette en bruger eller virksomhed registreres i tjenesten, men gennemføres manuelt af databehandleren. Det sker inden for 30 dage efter anmodningen. Databehandleren udleverer på anmodning en medarbejders positions- og tilstedeværelseshistorik som eksport, så den dataansvarlige kan besvare en anmodning om indsigt.
- Henvendelser fra registrerede videresendes til den dataansvarlige senest 3 arbejdsdage efter modtagelsen.
- Konsekvensanalyse: se Bilag D.6.3.

C.3.1. Oplysninger ved brud (Bestemmelse 10.4)

Databehandleren giver den dataansvarlige følgende, efterhånden som det bliver kendt: tidspunktet for bruddet og for opdagelsen, hvad der er sket, hvilke systemer og datakategorier der er berørt, et skøn over antallet af berørte registrerede og registreringer (herunder om positionsdata er berørt), de sandsynlige konsekvenser, hvad der er gjort og planlægges for at begrænse skaden, samt en kontaktperson.

C.4. Opbevaringsperiode/sletterutine

DATA	OPBEVARING OG SLETNING
BLE-observationer	Slettes automatisk efter 90 dage
Hændelser for ankomst og afgang	Slettes automatisk efter 180 dage
Aktuel tilstedeværelse pr. bruger (inkl. GPS)	Ingen tidsgrænse. Overskrives ved næste registrering

Værktøjs-, netværks- og prioritetsobservationer med bruger og GPS	Opbevares, så længe abonnementet løber
Bevægelseshistorik	Opbevares, så længe abonnementet løber
Aktivitetslog, udlån, anmeldelser, supportsager	Ingen tidsgrænse
Anmeldelser til forsikring	Rapporten sendes som PDF pr. e-mail og gemmes ikke i fillagringen. Anmeldelsen gemmes i databasen uden tidsgrænse
Rå RFID-scanninger i PostgreSQL/Timescale	Slettes automatisk efter 90 dage. Dagsopsummeringer bevares
RFID-scanninger i InfluxDB Cloud	Opbevares, så længe abonnementet løber
Fillagring	Slettede filer kan genskabes i 30 dage
Slettede brugere og virksomheder	Markeres som slettet. Endelig sletning sker manuelt efter anmodning (C.3)

Ved ophør sletter databehandleren den dataansvarliges oplysninger efter Bestemmelse 11.1 senest 90 dage efter ophøret og bekræfter sletningen skriftligt til den dataansvarliges kontaktperson. Sletningen udføres manuelt af databehandleren efter en skriftlig, intern sletteprocedure, som dækker database, fillagring, Firebase og RFID-tidsserier fra den dataansvarliges læsere i PostgreSQL. InfluxDB Cloud kan ikke slette enkelte læsers data; dér sætter databehandleren opbevaringstiden, så scanningerne fra den dataansvarliges afmeldte læsere udløber inden for fristen i dette afsnit. Kopier i backup forsvinder derefter af sig selv inden for 7 dage (database) og 30 dage (blødt slettede filer). Samme procedure bruges, når den dataansvarlige anmoder om sletning af virksomheden i tjenesten. Før sletning kan den dataansvarlige bede om en eksport.

C.5. Lokaltet for behandling

Behandling af de af Bestemmelserne omfattede personoplysninger kan ikke uden den dataansvarliges forudgående skriftlige godkendelse ske på andre lokaliteter end følgende:

- Microsoft Azure, region North Europe (Irland)
- Google Cloud/Firebase, EU-regioner (europe-west3)
- InfluxDB Cloud, AWS Frankfurt (eu-central-1)
- Stackhero (EU)
- Mailgun EU og Grafana Cloud eu-north-0 (Stockholm)
- Underdatabehandlere i tredjelande efter Bilag B og C.6
- Databehandlerens medarbejders arbejdssteder i EU/EØS – kun fjernadgang, ingen lokal lagring af kundedata

C.6. Instruks vedrørende overførsel af personoplysninger til tredjelande

Den dataansvarlige instruerer databehandleren i at overføre personoplysninger til de underdatabehandlere i tredjelande, der er angivet i Bilag B, kun til de formål, der står dér:

MODTAGER	LAND	DATA	OVERFØRSELGRUNDLAG (KAPITEL V)
Anthropic Ireland, Limited (behandling i USA)	USA	Billeder og tekst fra AI-briller, feedback og supportsager	Art. 46, stk. 2, litra c: SCC i Anthropics DPA
OpenAI Ireland Ltd. (behandling i USA)	USA	Tale fra appen	Art. 46, stk. 2, litra c: SCC i OpenAIs DPA

650 Industries, Inc. (Expo) og Google (FCM)	USA	Push-token og beskedtekst	Art. 45: DPF. Desuden SCC i leverandørernes vilkår
GitHub, Inc.	USA	Supportsager og feedback	Art. 45: DPF. Desuden SCC i GitHub's DPA
Netlify, Inc.	USA/globalt	Trafik til app.trackrs.dk	Art. 45: DPF. Desuden SCC i Netlify's DPA
InfluxData Inc., Mailgun Technologies, Inc., Raintank, Inc. (Grafana Labs)	USA	Mulig adgang til data, der opbevares i EU	Art. 45: DPF. Desuden SCC i leverandørernes DPA
Microsoft (support- og drifts adgang)	Tredjelande	Mulig adgang til data i EU-regioner	Art. 46, stk. 2, litra c: SCC i Microsofts DPA
Google (support- og drifts adgang)	USA	Mulig adgang til data i EU-regioner	Art. 45: DPF (Google LLC). Desuden SCC i Googles DPA

Databehandleren kontrollerer mindst én gang om året og før hver ny version, at certificeringen på dataprivacyframework.gov stadig er aktiv, og at leverandørens DPA indeholder SCC.

Hvis den dataansvarlige ikke i disse Bestemmelser eller efterfølgende giver en dokumenteret instruks vedrørende overførsels af personoplysninger til et tredjeland, er databehandleren ikke berettiget til inden for rammerne af disse Bestemmelser at foretage sådanne overførsler.

C.7. Procedurer for den dataansvarliges revisioner, herunder inspektioner

Databehandleren besvarer en gang om året uden betaling den dataansvarliges skriftlige spørgeskema om behandlingssikkerhed og overholdelse af Bestemmelserne inden for 30 dage. Databehandleren udsteder ikke en uafhængig revisionserklæring (fx ISAE 3000).

Den dataansvarlige eller en uafhængig revisor, som den dataansvarlige bemyndiger, og som har tavshedspligt, kan desuden foretage en inspektion, herunder af de systemer der bruges til behandlingen, med 30 dages skriftligt varsel og inden for normal arbejdstid. Inspektionen kan også gennemføres, når den dataansvarlige finder det nødvendigt, fx efter et brud. Den dataansvarlige afholder sine egne udgifter. Databehandleren afsætter den nødvendige tid, jf. Bilag D.4.

C.8. Procedurer for revisioner, herunder inspektioner, med behandling af personoplysninger, som er overladt til underdatabehandlere

Databehandleren fører tilsyn med underdatabehandlerne ved mindst én gang om året at gennemgå deres offentliggjorte revisionserklæringer (fx ISO 27001, SOC 2 Type II), deres databehandleraftaler og deres lister over underleverandører. Hvis der ikke findes en erklæring, sker tilsynet ved at gennemgå leverandørens dokumentation. Databehandleren sender på anmodning dokumentation for tilsynet til den dataansvarlige. Den dataansvarlige kan anfægte metoden og bede om et supplerende tilsyn.

BILAG D – PARTERNES REGULERING AF ANDRE FORHOLD

D.1. Elektronisk indgåelse (underskrift)

D.1.1. Bestemmelserne indgås elektronisk. Når en bruger med administratorrolle i Trackrs accepterer databehandleraftalen for [virksomhedens navn], udgør det den dataansvarliges underskrift efter Bestemmelse 14.1. Databehandlerens underskrift består i, at databehandleren har offentliggjort og stillet netop denne version til accept. Aftalen er dermed indgået skriftligt i elektronisk form, jf. databeskyttelsesforordningens artikel 28, stk. 9.

D.1.2. Brugeren, der accepterer, bekræfter at have bemyndigelse til at forpligte den dataansvarlige.

D.1.3. Databehandleren registrerer for hver accept: aftaleversion, en kontrolsum af den accepterede tekst (herunder Bilag B.1), tidspunkt (UTC), brugerens navn og e-mail, den oplyste IP-adresse og brugerens browser (user agent). Registreringen er knyttet til virksomheden. Registreringen er gemt uforanderligt, så længe Bestemmelserne gælder, og i 5 år derefter som dokumentation. Registreringen er ikke omfattet af sletningen efter Bestemmelse 11.1, da den er databehandlerens egen dokumentation for aftalen.

D.1.4. Den accepterede version kan til enhver tid hentes som PDF i indstillingerne i Trackrs på web. Ønsker du den på anden måde, kontakt os på privacy@trackrs.dk. Begge parter opbevarer dermed Bestemmelserne elektronisk, jf. Bestemmelse 2.10.

D.2. Hovedaftalen og nye versioner

D.2.1. "Hovedaftalen" er abonnementsvilkårene for Trackrs på <https://trackrs.dk/da/terms.html>. Spørgsmål om erstatningsansvar, betaling og opsigelse reguleres i hovedaftalen, så længe det ikke strider mod Bestemmelserne, jf. Bestemmelse 13.1.

D.2.2. Ændringer af Bilag B sker efter Bestemmelse 7.3 og Bilag B.2. Andre ændringer af Bestemmelserne eller bilagene kræver en ny version, som den dataansvarlige skal acceptere efter D.1. Databehandleren varslers en ny version med mindst 30 dage pr. e-mail til administratorerne. Indtil den nye version er accepteret, gælder den senest accepterede version.

D.2.3. Den dataansvarlige kan til enhver tid ændre sin kontaktperson efter Bestemmelse 15 ved at skrive til privacy@trackrs.dk. Underretninger efter Bestemmelse 7.3 og 10 sendes desuden til alle brugere med administratorrolle i virksomheden.

D.2.4. Den dataansvarlige kan til enhver tid give supplerende instruks (Bestemmelse 4.1) skriftligt til privacy@trackrs.dk. Databehandleren bekræfter modtagelsen skriftligt, og instruksens opbevares sammen med den accepterede aftale.

D.2.5. Eksisterende kunder får besked pr. e-mail til virksomhedens administratorer. For dem gælder version 1.1 fra 1. december 2026, medmindre de gør indsigelse inden da. Nye kunder accepterer ved oprettelse, og for dem gælder version 1.1 fra accepten.

D.3. Instruks, der er i strid med reglerne

D.3.1. Underretter databehandleren efter Bestemmelse 4.2, kan databehandleren udsætte den del af behandlingen, som instruksens angår, indtil den dataansvarlige har bekræftet, ændret eller trukket instruks tilbage. Databehandleren er ikke ansvarlig for følgerne af en sådan udsættelse.

D.4. Bistand, der rækker ud over standardfunktionerne

D.4.1. Bistand efter Bestemmelse 9 ydes uden særskilt betaling, i det omfang den kan ydes med funktionerne i Trackrs eller med den manuelle hjælp, der er beskrevet i Bilag C.3. Omfattende bistand ud over dette (fx en konkret konsekvensanalyse for den dataansvarlige eller en revision på stedet) kan faktureres efter medgået tid til databehandlerens gældende timepris, som oplyses, før arbejdet sættes i gang. Bistand, der skyldes databehandlerens eget brud på Bestemmelserne, faktureres ikke.

D.5. Lovvalg og værneting

D.5.1. Bestemmelserne er underlagt dansk ret. Tvister afgøres ved Retten i Roskilde som første instans.

D.6. Registrering af medarbejderes position og tilstedeværelse

D.6.1. Den dataansvarliges ansvar. Den dataansvarlige afgør, om tilstedeværelse og positionsregistrering skal bruges, og har ansvaret for, at der er et behandlingsgrundlag. Det er typisk databeskyttelseslovens § 12, stk. 1, hvis registreringen er en kontrolforanstaltning efter en kollektiv aftale, og ellers artikel 6, stk. 1, litra f. Den dataansvarlige skal:

a) informere medarbejderne om formål, omfang og brug af oplysningerne senest når registreringen tages i brug (artikel 13). Er virksomheden omfattet af en aftale om kontrolforanstaltninger, skal den også varsle efter aftalen.

b) sikre, at positionsdata ikke bruges til andre formål end dem, der er oplyst, fx ikke til at overvåge medarbejderes adfærd

eller opholdssted uden for arbejdet

c) vurdere, om der skal laves en konsekvensanalyse (se D.6.3)

d) sikre, at medarbejdere ikke registreres uden for arbejdstid. Appen kan på iOS have tilladelsen "Altid" og har ingen indbygget afgrænsning til arbejdstid. Den dataansvarlige skal derfor selv fastlægge og oplyse, hvornår medarbejderne skal have lokationstilladelsen slået til.

D.6.2. Databehandlerens bistand. Databehandleren stiller følgende til rådighed:

a) en skabelon til medarbejderinformation (nedenfor)

b) en beskrivelse af hvilke positionsdata der indsamles, hvornår og hvor længe de gemmes (Bilag A.2, A.3 og C.4)

c) oplysning om, hvordan registreringen kan begrænses: den enkelte medarbejder kan slå lokationstilladelsen fra i telefonens indstillinger, og deltagelse i netværksobservationer kan slås fra pr. bruger. Der findes ingen indstilling, der slår tilstedeværelse fra for hele virksomheden

d) svar på den dataansvarliges spørgsmål til brug for konsekvensanalysen inden for 30 dage

D.6.3. Konsekvensanalyse. Datatilsynets liste over behandlinger, der altid kræver en konsekvensanalyse, omfatter behandling af lokationsdata, når mindst ét yderligere kriterium fra WP248 er opfyldt (pkt. 3). Systematisk overvågning og ansatte som registrerede er sådanne kriterier. Den dataansvarlige bør derfor gå ud fra, at en konsekvensanalyse er påkrævet, før tilstedeværelse med telefonens position tages i brug.

SKABELON TIL MEDARBEJDERINFORMATION

(Ikke en del af aftalen. Findes også på GDPR-siden. Den dataansvarlige udfylder felterne i [] og udleverer skabelonen, senest når funktionen tages i brug.)

Sådan bruger [Virksomhed] Trackrs

[Virksomhed], CVR [nr.], bruger Trackrs til at holde styr på værktøj og udstyr. Trackrs leveres af Rasmussen Solutions ApS, som behandler oplysningerne på vores vegne.

Hvad registreres: dit navn, e-mail og rolle, hvilket værktøj du har lånt eller flyttet, og hvornår. Hvis [Virksomhed] bruger tilstedeværelse, bruger Trackrs-appen din telefons position til at registrere, hvornår du kommer til og forlader vores lokationer: [liste: lager, værksted, byggepladser ...]. Appen kan registrere i baggrunden, når du har givet tilladelse til det.

Formål: at finde værktøj, forebygge tyveri og vide, hvilket udstyr der er på hvilken lokation. Oplysningerne bruges ikke til [at bedømme din arbejdsindsats / at følge dig uden for arbejdstid].

Behandlingsgrundlag: [databeskyttelseslovens § 12, stk. 1 (aftale om kontrolforanstaltninger) / databeskyttelsesforordningens art. 6, stk. 1, litra f – vores legitime interesse i at beskytte og planlægge brugen af vores udstyr].

Hvem ser oplysningerne: [roller]. Leverandøren og dennes underleverandører, se [link til GDPR-siden].

Hvor længe: ankomst- og afgangshændelser 180 dage. BLE-observationer 90 dage. Udlånshistorik [periode].

Dine muligheder: du kan slå lokationstilladelsen fra i telefonens indstillinger [konsekvens: ...]. Du har ret til indsigt, berigtigelse, sletning, begrænsning og indsigelse. Kontakt [navn/e-mail]. Du kan klage til Datatilsynet, www.datatilsynet.dk.