



Mall för den Personuppgiftsansvarigs Instruktion för Behandling av Personuppgifter vid utförande av trafikuppdrag

1. Ändamål med Behandlingen

Personuppgiftsbiträdet åtar sig att endast behandla Personuppgifter som denne får tillgång till under Avtalet och/eller Personuppgiftsbiträdesavtalet för Personuppgiftsansvarigs räkning, för att:

[Ange för vilka ändamål som Personuppgiftsbiträdet behandlar Personuppgifterna.

Exempel:

- *Ta emot och hantera kundsupportärenden (exempelvis kvarglömda väskor eller andra frågor kopplat till resor);*
- *Hantera bussförarens tillgång till Personuppgiftsansvarigs lokaler;*
- *Utföra kamerabevakning i bussar för att bl.a. förebygga, förhindra och/eller utreda brott eller annan skadegörelse;*
- *Hantera resebiljetter;*
- *Planera och utföra resor för skolbarn.]*

För undvikande av tvivel noteras det att, för det fall Personuppgiftsbiträdet behandlar Personuppgifter som denne får tillgång till i egenskap av Personuppgiftsbiträde under Avtalet och/eller Personuppgiftsbiträdesavtalet, för annat ändamål än att uppfylla sina åtaganden under Avtalet och/eller Personuppgiftsbiträdesavtalet, ska Personuppgiftsbiträdet i förhållande till sådan personuppgiftsbehandling betraktas som Personuppgiftsansvarig och åtar sig i så fall att tillse att Behandlingen uppfyller gällande Dataskyddslagstiftning.

2. Behandlingen omfattar följande kategorier av Behandling

Personuppgiftsbiträdet kommer att utföra följande Behandling för Personuppgiftsansvarigs räkning:

[Ange vilka typer av Behandlingar som Personuppgiftsbiträdet utför för Personuppgiftsansvarigs räkning i syfte att fullgöra Behandlingens ändamål.

Exempel:

- *Hantera och besvara kundsupportärenden;*
- *Lagra och hantera bussförarens åtkomst till lokaler;*
- *Lagra, analysera och/eller få tillgång till Personuppgifter i samband med supporttjänster eller IT-system;*
- *Lagra och hantera åtkomst till bildmaterial från kamerabevakning.]*



3. Behandlingen omfattar följande kategorier av Registrerade

Personuppgiftsbiträdet kommer att behandla Personuppgifter för följande kategorier av Registrerade:

[Ange vilka kategorier av Registrerade vars Personuppgifter Personuppgiftsbiträdet har åtkomst till och kommer Behandla.

Exempel:

- *Kunder/Resenärer;*
- *Anställda hos Personuppgiftsbiträdet;*
- *Anställda hos Personuppgiftsansvarig;*
- *Konsulter;*
- *Elever/skolbarn;*
- *Vårdnadshavare.]*

4. Behandlingen omfattar följande kategorier av Personuppgifter

Behandlingen omfattar följande kategorier av Personuppgifter:

[Ange här vilka kategorier av Personuppgifter som Behandlas.

Exempel:

- *Namn;*
- *Kontaktuppgifter såsom email, adress, telefonnummer;*
- *Bildmaterial från kamerabevakning;*
- *AnställningsID/ FörarID;*
- *Lokaliseringsuppgifter.]*

5. Plats för Behandling

Personuppgiftsbiträdet kommer att Behandla Personuppgifter på följande platser:

[Ange plats för Behandlingen, d.v.s. var Personuppgiftsbiträdet får åtkomst till Personuppgifterna och var dessa i övrigt Behandlas och om Personuppgifterna kommer att lagras hos Personuppgiftsansvarig eller hos Personuppgiftsbiträdet.

Exempel:

- *EU/EES, särskilt*
 - *Sverige (Personuppgiftsansvarigs anläggning, och*
 - *Nederländerna (Personuppgiftsbitrådets server).*

Personuppgiftsbiträdet får inte utan Personuppgiftsansvarigs skriftliga medgivande föra över och/eller Behandla Personuppgifter i land utanför EU/EES.

6. Gallring, radering och återlämning

Enligt Dataskyddslagstiftningen ska Personuppgifter gallras så snart ändamålen med Behandlingen för vilka de samlades in har fullgjorts, såvida det inte följer av krav i annan lagstiftning att Personuppgifter måste sparas under viss tid innan de gallras.

Personuppgiftsbiträdet ansvarar för att löpande gallra (d.v.s. radera) Personuppgifter som den har tillgång till och förvarar på egna (eller på Underleverantörers) servrar vid



utförandet av Avtalet och/eller Personuppgiftsbiträdesavtalet. Gallring ska ske automatiskt eller manuellt. Gallring av Personuppgifter som Personuppgiftsbiträdet inte längre behöver för att uppfylla sina skyldigheter enligt Avtalet och/eller Personuppgiftsbiträdesavtalet ska raderas minst en gång om året, eller oftare om det är lämpligt, om inte andra instruktioner framgår av denna Instruktion.

[Finns behov av anpassning av gallringstid kan det anges nedan.]

Exempel:

- Bildmaterial från kamerabevakning i bussar ska löpande gallras efter X dagar;
- Personuppgifter från kundtjänstvärderna ska raderas X dagar efter avslutat ärende;
- Personuppgifter från tillgångskonstroll till lokaler ska raderas X dagar efter trafikuppdragets upphörande.]

7. Underbiträden

Personuppgiftsansvarig har godkänt att Personuppgiftsbiträdet anlitat följande Underbiträden:

[Ange här om, och så fall vilka, Underbiträden som Personuppgiftsbiträdet har anlitat, vilken tjänst Underbiträdet utför samt var Behandlingen sker.]

Exempel:

- Underbiträde 1 AB, levererar molntjänst för ärendehanteringssystem för kundtjänst, Sverige och Irland;
- Underbiträde 2 AB, utför trafikuppdrag på uppdrag av Personuppgiftsbiträdet, Sverige;
- Underbiträde 3 AB, levererar ersättningstrafik på uppdrag av Personuppgiftsbiträdet, Sverige.]

8. Tekniska och organisatoriska säkerhetsåtgärder

Personuppgiftsbiträdet ska vid var tid uppfylla nedan tekniska och organisatoriska säkerhetsåtgärder och fortlöpande säkerställa att säkerheten i samband med Behandlingen medför en lämplig nivå av konfidentialitet, integritet, tillgänglighet och motståndskraft, bl.a. genom att, där nödvändigt;

- Personuppgiftsbiträdet ska uppfylla de krav som stipuleras av Dataskyddslagstiftningen, den Personuppgiftsansvarigas informationsklassning samt i förekommande fall egen informationsklassning;
- Personuppgiftsbiträdet ska aktivt arbeta med och utbilda kring sitt informations säkerhetsarbete internt i syfte att dessa krav efterlevs;
- Personuppgiftsbiträdet ska tillse att tekniska säkerhetsåtgärder för åtkomsthantering (både fysisk och systemmässigt), kryptering (både vid överföring och i vila), distansarbete (så som tvåfaktorsautentisering och säker anslutning) samt säkerhetskopiering implementeras i paritet till skyddsvärdet hos de Personuppgifter som behandlas;
- Personuppgiftsbiträdet ska kunna uppvisa dokumenterade riktlinjer och instruktioner som påvisar organisatoriska och tekniska säkerhetsåtgärder;
- Personuppgiftsbiträdet ska ha dokumenterade rutiner för att löpande kunna upptäcka och hantera Personuppgiftsincidenter;



- Personuppgiftsbiträdet ska ha dokumenterade och implementerade rutiner för att hantera en Registrerads förfrågan om att tillvarata sina rättigheter (såsom registerutdrag);
- Personuppgiftsbiträdet ska granska och kontrollera de interna organisatoriska och tekniska säkerhetsåtgärderna periodiskt samt validera dess lämplighet.

[Ange här om det finns tekniska och organisatoriska krav för särskilt angivna Behandlingar.
Exempel:

- *Kamerabevakning i bussar:*
 - *Överföringar av inspelat material ska ske via krypterade kanaler;*
 - *Åtkomst till inspelat material ska loggas och kunna följas upp;*
 - *Uttag och utlämnande av inspelat material ska följa tydliga rutiner samt vara spårbart.]*

9. Loggning

Vid Behandling av Personuppgifter gäller följande för Loggning:

[Ange här vilka regler som gäller för Loggning och åtkomst till Personuppgifter.
Exempel:

- *Endast personal hos Personuppgiftsbiträdet med behov till det ska ha åtkomst till Personuppgifter;*
- *Åtkomst till lokaler som kan ge tillgång till Personuppgifter ska loggas och granskas vid behov;*
- *Åtkomst och förändring av Personuppgifter i system ska loggas och granskas vid behov;*
- *Loggar ska som minimum påvisa vem åtkomsten härför sig till, när den skedde samt vad som förändrades.]*

10. Övriga Instruktioner angående Behandling av Personuppgifter som utförs av Personuppgiftsbiträdet

[Här kan det skrivas in övriga instruktioner som inte har täcks av ovan avsnitt.
Exempel:

- *Personuppgiftsincidenter ska rapporteras till exempel@mail.com.]*