# Instruktion

## 1. Instruktionen

Denna instruktion är en bilaga till personuppgiftsbiträdesavtalet avseende de behandlingar av personuppgifter som [Företaget] utför för Statens haverikommissions (SHK) räkning. Definitioner och termer häri har samma betydelse som i personuppgiftsbiträdesavtalet, om inte omständigheterna uppenbart föranleder annat.

## 2. Ändamålet med behandlingen

[Ange ändamålet med behandlingen]

## 3. Kategorier av registrerade

[Ange kategorier av registrerade t.ex. personal, andra myndigheter, leverantörer].

## 4. Typ av personuppgifter som behandlas

[Ange typ av personuppgifter t.ex. namn, personnummer, postadress, e-postadress, telefonnummer, foton, video- och ljudupptagningar].

## 5. Känsliga personuppgifter (i förekommande fall)

[Ange vilka typer av känsliga personuppgifter som kan förekomma t.ex. hälsa, facklig tillhörighet].

## 6. Särskilda instruktioner rörande behandlingen

[Om inga sådana finns skriv ”Vid detta avtalstecknande finns inga särskilda instruktioner]

## 7. Behandlingens varaktighet

Behandlingen varar till dess att affärsavtalet mellan SHK och [Företaget] upphör att gälla.

## 8. Godkända underbiträden

| *Namn* | *Typ av behandling* | *Plats för behandling* |
|---|---|---|
| | | |
| | | |

## 9. Tekniska och organisatoriska säkerhetsåtgärder

I det följande redogörs för de säkerhetsåtgärder som Personuppgiftsbiträdet, samt i tillämpliga fall underbiträden, ska vidta vid behandling av personuppgifter för Personuppgiftsansvariges räkning. Utöver vad som framgår av affärsavtalet mellan Personuppgiftsansvarig och Personuppgiftsbiträdet samt personuppgiftsbiträdesavtalet ska Personuppgiftsbiträdet även vidta de åtgärder som framgår nedan. Personuppgiftsbiträdet ska tillse att underbiträden vidtar motsvarande åtgärder.

9.1 Generellt ska Personuppgiftsbiträdet vidta följande åtgärder vid sin behandling av personuppgifter för Personuppgiftsansvariges räkning.

a) Vidta nödvändiga åtgärder för att skydda personuppgifterna mot förstöring, ändringar och otillåten spridning.
b) Vidta nödvändiga åtgärder för att förhindra obehörig åtkomst till personuppgifterna.
c) Begränsa antalet användare med åtkomst till personuppgifterna till de personer som behöver ha tillgång till uppgifterna för att utföra sina arbetsuppgifter.
d) Säkerställa den fysiska säkerheten för personuppgifterna.
e) Alltid ha återställnings – och katastrofplaner implementerade och testade.
f) Följa SHK:s säkerhetsanvisningar.

9.2 När datorutrustning och löstagbara datamedier hos Personuppgiftsbiträdet inte står under uppsikt ska utrustningen och medierna låsas in för att skyddas mot obehörig användning, påverkan och stöld. I annat fall ska personuppgifterna krypteras.

9.3 För det fall eventuella bärbara datorer eller dylik utrustning används vid behandlingar ska personuppgifterna på fasta och löstagbara lagringsmedier alltid vara krypterade.

9.4 Personuppgifterna ska regelbundet överföras till säkerhetskopior. Kopiorna ska förvaras avskilt och väl skyddade så att personuppgifterna kan återskapas efter en störning. Personuppgiftsbiträdet ska ha en rutin för test av återläsning.

9.5 Ett tekniskt system för behörighetskontroll ska styra åtkomsten till personuppgifterna hos Personuppgiftsbiträdet. Behörigheten ska begränsas till dem som behöver ha tillgång till uppgifterna för att utföra sitt arbete. Användaridentitet och lösenord ska vara personliga och får inte överlåtas

till någon annan. Det ska finnas rutiner för tilldelning och borttagande av behörigheter.

9.6 Åtkomst till personuppgifter ska kunna följas upp i efterhand genom en logg eller liknande underlag. Underlaget ska kunna kontrolleras av Personuppgiftsbiträdet och återrapporteras till den Personuppgiftsansvarige.

9.7 Anslutning för extern datakommunikation ska skyddas med sådan teknisk funktion som säkerställer att uppkopplingen är behörig.

9.8 För åtkomst till känsliga och integritetskänsliga personuppgifter krävs tvåfaktorsautentisering.

9.9 Personuppgifter som överförs via datorkommunikation utanför lokaler som kontrolleras av Personuppgiftsbiträdet ska skyddas med kryptering.

9.10 När fasta eller löstagbara lagringsmedier som innehåller personuppgifter inte längre ska användas för sitt ändamål ska personuppgifterna raderas på sådant sätt att de inte kan återskapas.

9.11 När reparation och service av datorutrustning, vilken används för att lagra Personuppgiftsansvariges personuppgifter, utförs av annan än personuppgiftsbiträdet, ska avtal som reglerar säkerhet och sekretess träffas med serviceföretaget.

9.12 Vid servicebesök ska service ske under Personuppgiftsbiträdets överinseende. Är detta inte möjligt ska lagringsmedier som innehåller personuppgifter avlägsnas.

9.13 Service via fjärrstyrd datorkommunikation får endast ske via säker anslutning och efter säker elektronisk identifiering av den som utför service. Servicepersonal ska ges åtkomst i systemet endast vid servicetillfället. Finns separat kommunikationsingång för service ska den vara stängd när service inte pågår.

9.14 Den Personuppgiftsansvarige har rätt att utföra kontroller av att avtalade säkerhetsåtgärder faktiskt vidtas.