Bilaga 1 - Instruktion för hantering av Personuppgifter

Utöver vad som redan framgår av detta avtal ska personuppgiftsbiträdet även följa nedanstående instruktioner:
1. Ändamål, föremålet och arten
Avtal om pensionsadministration (Avtalet) har tecknats mellan personuppgiftsansvarig (Arbetsgivare/S och personuppgiftsbiträdet (Pensionsadministratören).
Pensionsadministration innebär att Pensionsadministratören för Arbetsgivarens räkning, administrerar Arbetsgivarens pensionsutfästelser enligt de pensionsbestämmelser som gäller för Arbetsgivaren.
2. Behandlingen omfattar följande typer av Personuppgifter
Personuppgiftsbiträdet kommer under avtalet behandla följande typer av personuppgifter:
- Namn
Kontaktuppgifter
Personnummer
- Anställningstid
Ledighetsperioder
Tidpunkter för sjuk- och aktivitetsersättning
Yrke
Tidpunkt för dödsfall
Pensionsgrundande lön
Arvode
- Valt försäkringsbolag för avgiftsbestämd pension
Premier till valt försäkringsbolag
- Allmän pension
- Uppgifter för preliminär skatt
Inloggningsuppgifter och uppgift för behörighetskontroller och loggning
När Personuppgiftsbiträdet behandlar tidpunkt för sjuk och aktivitetsersättning sa är det en behandling av särskilda kategorier av personuppgifter enligt artikel 9 i GDPR.
3. Behandlingen omfattar kategorier av Registrerade
Personuppgiftsbiträdet kommer att under avtalet behandla personuppgifter gällande följande kategorier av registrerade
.
arbetstagare som r eller har varit anställd hos Arbetsgivaren och för vilka Arbetsgivarens pensionsbestämmelser gäller
• pensionstagare, för vilka Arbetsgivarens pensionsbestämmelser gäller
• förtroendevalda, för vilka Arbetsgivarens pensionsbestämmelser gäller
4. Ange särskilda hanteringskrav vad gäller Behandling av Personuppgifter som utförs av Personuppgiftsbiträdet/biträdena
Enligt Dataskyddslagstiftningen ska personuppgifter tas bort (gallras) så snart det inte längre är nödvändigt med hänsyn till ändamålen med behandlingen.

De personuppgifter som Personuppgiftsbiträdet behandlar inom ramen för Avtalet ska under avtalstiden gallras en gång varje kalenderår för personuppgifter som inte längre behövs för att säkerställa ändamålen med behandlingen.
Särskilda krav på hantering rörande gallring, utöver vad som anges ovan och i punkt 18.2 i Personuppgiftsbiträdesavtalet, gäller då Personuppgiftsansvarig valt att byta leverantör. Detta

för att kunna säkerställa åtagandet mot arbetsgivaren (Personuppgiftsansvarig) vad aver överföringen av uppgifter till ny leverantör.
Senast trettio (30) dagar räknat från den tidpunkt uppsägning gjorts enligt PUB-avtal, punkt 16.1 ska personuppgifterna vara avskilda så att de fortsatt är tillgängliga men endast för ett begränsat fåtal behöriga hos Personuppgiftsbiträdet.
Personuppgifterna ska finna tillgängliga enligt ovan under ett ar efter överföring till ny leverantör skett eller under längre tid om rutin för överförande av personuppgifter till ny leverantör kräver
det.
På begäran från Personuppgiftsansvarig ska Personuppgifterna kunna sparas under en längre tid.
5. Lokalisering och överföring av Personuppgifter till Tredje land
Personuppgiftsbiträdet är skyldig att se till att all behandling av personuppgifter under Biträdesavtalet som utförs av Personuppgiftsbiträdet, på egen hand eller via underbiträden, sker inom EU/EES.
6. Övriga Instruktioner angående Behandling av personuppgifter som utförs av biträdet/biträdena
Om en registrerad hos arbetsgivaren har ansökt om registerutdrag ska Personuppgiftsbiträdet på begäran från den Personuppgiftsansvarige tillhandahålla den Personuppgiftsansvarige en kopia över de personuppgifter som behandlas om den sökande med anledning av Avtalet.
Om Personuppgiftsbiträdet direkt från en registrerad får en ansökan om registerutdrag som avser den behandling av personuppgifter som omfattas av Avtalet, ska Personuppgiftsbiträdet informera den registrerade om att det r den Personuppgiftsansvarige som ansvarar för personuppgiftsbehandlingen och därmed också registerutdragen samt hänvisa den sökande till den Personuppgiftsansvarige.

Bilaga 2 - Säkerhetsinstruktioner

Denna Bilaga 2 till Biträdesavtalet innehåller instruktioner till PUB och redogör för de tekniska och organisatoriska säkerhetsåtgärder som PUB ska vidta i enlighet med Biträdesavtalets punkt 5.

Fysisk säkerhet

Lämpliga och adekvata åtgärder ska vidtas för att säkerställa den fysiska säkerheten av it-utrymmen? såsom, men inte begränsat till, skalskydd, tillträdesskydd, brandskydd, skydd mot elavbrott, stöldskydd och skydd mot skadegörelse. De vidtagna åtgärderna ska säkerställa en skyddsnivå som minst motsvarar de skyddsnivåer som anges I bilaga 1 till MSB:s vägledning för fysisk informationssäkerhet i it-utrymmen.

Inventering av datorutrustning och system

Det ska föras en förteckning över datorutrustning och system som används för Behandling av Personuppgifter. Det ska finnas dokumenterade rutiner för löpande uppdatering av denna förteckning.

Åtkomstskydd

Datorutrustning och portabla lagringsmedier som inte står under uppsikt ska läsas in för att skyddas mot obehörig användning, påverkan och stöld. I annat fall ska Personuppgifter krypteras.

Datorer och mobila enheter

Medarbetares datorer ska låsas automatiskt vid inaktivitet och kräva starkt lösenord för uppläsning.

Antalet öppna kommunikationsportar i datorerna ska minimeras och brandväggar, antivirusprogram och säkerhetsuppdateringar ska installeras och uppdateras regelbundet. Hårddiskar tillhörande bärbara datorer ska alltid vara krypterade med tillräckligt stark nyckel. Lagringsminnen tillhörande mobila enheter ska krypteras med tillräckligt stark nyckel. Mobila enheter ska skyddas med ett tillräckligt starkt lösenord och raderas automatiskt om felaktigt lösenord matas in för många gånger. Det ska finnas möjlighet att radera Personuppgifter från mobila enheter via fjärr åtkomst. Behandling av Personuppgifter på mobila enheter ska begränsas enligt dokumenterade rutiner.

Medarbetare ska inte medges tillstånd att behandla Personuppgifter p privata datorer eller mobila enheter.

Autentisering

Inloggning i system ska ske via personlig an Sindaridentitet med lösenord. Lösenord ska vara tillräckligt starka och bytas regelbundet. Det ska inte vara tillåtet att överlåta eller dela inloggningsuppgifter med andra personer. Det ska föras ett register över användares inloggning i system. Vid en användares upprepade felaktiga inloggningsförsök i ett system ska användarkontot avaktiveras eller spärras för en definierat tid

Behörighetsstyrning

Medarbetares åtkomst till Personuppgifter ska styras av ett tekniskt system för behörighetskontroll.

Medarbetarna ska ges minsta möjliga åtkomst vid behandling av Personuppgifter. Endast

7 Med it-utrymmen avses samtliga lokaler som ar avsedda för IT-drift och förvarar IT-utrustning.

* MSB, 2013, Vägledning for fysisk informationssäkerhet 1 It-utrymmen, ISBN: 978-91-7383-401-8, tillgänglig på
https://www.msb.se/RibData/Filer/pdf/27280.pdf

PUB avtal KPA
medarbetare som behöver tillgång till Personuppgifter för sitt arbete ska ges åtkomst. Det ska finnas dokumenterade rutiner för tilldelning och borttagande av behörigheter.
Åtkomstkontroll
Åtkomst till Personuppgifter ska kunna kontrolleras i efterhand genom loggar. Loggarna ska kontrolleras regelbundet i syfte att upptäcka otillåten eller obehörig tillgång till Personuppgifter.
Servrar
Åtkomst till administrativa verktyg och gränssnitt p& servrar ska begränsas. Medarbetare som har administrativa rättigheter ska använda starka lösenord. Det ska inte vara tillåtet att överlåta eller dela inloggningsuppgifter med andra personer. Det ska finnas dokumenterade rutiner som säkerställer att viktiga uppdateringar för operativsystem och applikationer installeras omgående.
Nätverkssäkerhet
Nätverk ska skyddas mot externa angrepp och förlust av information. Trädlösa nätverk ska skyddas med kryptering. In- och utgående nätverkstrafik ska filtreras via exempelvis brandväggar. Mjukvara som regelbundet scannar nätverk för virus, trojaner och andra former av digitala intrång ska användas och hållas uppdaterad
Skydd mot skadlig kod och otillförlitliga program
Endast sådana program som formellt godkänts inom verksamheten ska få finnas i systemmiljön. Det ska finnas dokumenterade rutiner för att skydda system mot virus, trojaner och andra former av digitala intrång.
Säkerhetskopior
Personuppgifter ska regelbundet (minst en gång per dag) överföras till säkerhetskopior. Säkerhetskopiorna ska förvaras avskilt och väl skyddade så att Personuppgifter kan återskapas efter en störning. Det ska finna dokumenterade rutiner för säkerhetskopiering, återläsning av säkerhetskopior och test av återläsning av säkerhetskopior.
Datakommunikation
Anslutning för extern datakommunikation ska skyddas med sådan teknisk funktion som säkerställer att uppkopplingen är behörig. Personuppgifter som överförs via öppna nätverk (t.ex. internet) ska skyddas med kryptering.
Utplåning
Det ska finna dokumenterade rutiner som säkerställer att Personuppgifter kan raderas när de inte länge är nödvändiga för ändamålet och att de inte är möjliga att återskapa.
Reparation och service
När reparation och service av datorutrustning utförs av annan än PUB eller Underbiträde, ska kontrakt som reglerar säkerhet och sekretess träffas med serviceföretaget. Vid servicebesök ska servicen ske under PUB:s
eller Underbiträdets Överinseende. Är detta inte möjligt ska lagringsmedier som innehåller Personuppgifter avlägsnas.
Service via fjärrstyrd datakommunikation får endast ske efter säker elektronisk identifiering av den som utför servicen. Servicepersonal ska ges åtkomst I systemet endast vid

servicetillfället. Finns separat kommunikationsingång för service ska den vara stängd när service inte pågår.
Rapportering av personuppgiftsincidenter
Rutin för rapportering och uppföljning av personuppgiftsincidenter och andra säkerhetsincidenter ska finnas och följas. Rutinen ska omfatta hur information ska förmedlas, till vem rapportering ska ske och hur information sammanställs. Personuppgiftsincidenten ska följas upp och de brister i organisationen som lett till att personuppgiftsincidenten inträffat ska rättas till
Rutin för att omgående underrätta PUA vid misstanke om eller konstaterad personuppgiftsincident ska finnas. PUB ska ha förmågan att återställa tillgängligheten och åtkomsten till Personuppgifter i rimlig tid vid en inträffad personuppgiftsincident.
Rapportering av funktionsfel och brister
Det ska finnas dokumenterade rutiner för rapportering av fel, säkerhetsmässiga svagheter, brister och ändringsförslag. I rutinen ska det vara fastställt till vem och hur rapportering ska ske
Driftdokumentation
Dokumentation som beskriver den dagliga driften av system ska vara av tillräcklig kvalitet för att garantera upprätthållandet av tillgängligheten.
Separation
Personuppgifterna ska logiskt separeras från personuppgifter som PUB behandlar på uppdrag av andra än PUA.
Pseudonymisering
Personuppgifter ska i möjligaste mån pseudonymiseras."

Utbildning av personal
De krav som gäller för medarbetare med tillgång till system ska vara definierade av systemägaren.
Kraven ska avse såväl säkerhet som kompetens och ska vara dokumenterade och kommunicerade.
Medarbetare ska regelbundet (minst en gång per år) utbildas inom dataskydd. Nyanställda medarbetare ska genomgå utbildning inom dataskydd innan de får åtkomst till Personuppgifter.
Ytterligare åtgärder
PUB ska vidta alla ytterligare tekniska och organisatoriska säkerhetsåtgärder som krävs enligt Tillämplig dataskyddslag eller annan författning, beslut från behörig tillsynsmyndighet, gällande administrativ praxis och rättspraxis. Sådana ytterligare åtgärder ska också vidtas om detta krävs på grund av behandlingens art, omfattning, sammanhang och ändamål samt riskerna för Registrerades fri- och rättigheter.
Dokumentation av åtgärder
Genomförandet av samtliga säkerhetsåtgärder enligt denna bilaga 2 ska dokumenteras och tillhandahållas PUA på begäran.