BÄSTA LIVSPLATSEN
Region Halland

DN

Personuppgiftsbiträdesavtal mellan personuppgiftsansvarig och personuppgiftsbiträde avseende Integrationsförvaltning, DNRGS160253

PARTER

Personuppgiftsansvarig (**"PUA"**)
Regionstyrelsen Region Halland
Box 517
301 80 Halmstad
Organisationsnummer 232100-0115

Driftnämnden Ambulans diagnostik och hälsa
Långgatan 32
302 49 Halmstad
Organisationsnummer 232100-0115

Driftnämnden Hallands sjukhus
Hallands sjukhus Halmstad
301 85 Halmstad
Organisationsnummer 232100-0115

Driftnämnden Kultur och skola
Box 517
301 80 Halmstad
Organisationsnummer 232100-0115

Driftnämnden Närsjukvård
Box 1243
432 17 Varberg
Organisationsnummer 232100-0115

Driftnämnden Psykiatri
Träslövsvägen
432 81 Varberg
Organisationsnummer 232100-0115

Driftnämnden Regionservice
Box 517
301 80 Halmstad
Organisationsnummer 232100-0115

Personuppgiftsbiträde ("PUB")
Contica AB
Mässans gata 18
402 24 Göteborg
Organisationsnummer 556798-9347

PUA och PUB benämns även som **"Part"** och tillsammans **"Parterna"**.

1 INNEHÅLL OCH SYFTE

1.1 Mellan PUA och PUB har avtal tecknats avseende tjänster (**"Tjänsteavtalet"**) som PUB ska tillhandahålla PUA i egenskap av personuppgiftsbiträde. De avtalade tjänsterna innebär att PUB behandlar personuppgifter för PUA:s räkning, i omfattning som regleras i Tjänsteavtalet och detta personuppgiftsbiträdesavtal (**"Biträdesavtalet"**).

1.2 Enligt Tillämplig dataskyddslag, se punkt 2.5 nedan, ska behandling av personuppgifter utförd av ett personuppgiftsbiträde för en personuppgiftsansvarigs räkning regleras i avtal. Med anledning därav har Parterna ingått Biträdesavtalet.

1.3 Syftet med Biträdesavtalet är att tillse att PUB:s behandling av personuppgifter för PUA:s räkning sker i enlighet med Tillämplig dataskyddslag, myndighetsbeslut och PUA:s instruktioner.

1.4 Biträdesavtalet utgör bilaga till Tjänsteavtalet. Vid händelse av motstridiga bestämmelser ska Biträdesavtalet ges företräde.

2 DEFINITIONER

2.1 Med "Personuppgift" eller "Personuppgifter" avses nedan all slags information som direkt eller indirekt kan hänföras till en fysisk person som är i livet och som behandlas för PUA:s räkning.

2.2 Med "Registrerad" avses den fysiska person som Personuppgift avser.

2.3 Med "Behandling" eller "Behandla" avses åtgärd eller kombination av åtgärder beträffande Personuppgifter, oberoende av om de utförs automatiserat eller ej, såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring.

2.4 Med "Underbiträde" avses fysisk eller juridisk person, myndighet eller annat organ som anlitas av PUB för Behandling av Personuppgifter.

2.5 Med "Tillämplig dataskyddslag" avses Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av

personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning) med tillhörande genomförandeförfattningar samt all annan eventuell lagstiftning (inklusive förordningar och föreskrifter) som är tillämplig på Behandling av Personuppgifter, såsom denna kan komma att förändras över tid.

2.6 Begrepp och uttryck som rör personuppgifter och personuppgiftsbehandling och som inleds med gemen, t.ex. "personuppgiftsansvarig", "personuppgiftsbiträde", "personuppgiftsincident" etc., ska ges den betydelse som anges i Tillämplig dataskyddslag.

3 PERSONUPPGIFTSANSVARIGS ANSVAR

3.1 PUA är personuppgiftsansvarig för all Behandling av Personuppgifter i enlighet med Tillämplig dataskyddslag.

3.2 PUA åtar sig att utforma skriftliga instruktioner för att PUB och eventuella Underbiträden ska kunna fullgöra sitt uppdrag enligt Biträdesavtalet.

3.3 PUA:s instruktioner till PUB avseende Behandlingens art och ändamål, varaktighet, typen av Personuppgifter och kategorier av Registrerade framgår av *Bilaga* 1 till Biträdesavtalet.

3.4 PUA åtar sig att utan dröjsmål informera PUB om förändringar i Behandling av Personuppgifter vilka påverkar PUB:s skyldigheter enligt Tillämplig dataskyddslag eller annan relevant lagstiftning.

4 PERSONUPPGIFTSBITRÄDETS ÅTAGANDEN

4.1 PUB ska endast Behandla Personuppgifter i enlighet med Biträdesavtalet, Tjänsteavtalet och enligt vid var tid gällande dokumenterade instruktioner från PUA.

4.2 Vid Behandling av Personuppgifter ska PUB följa Tillämplig dataskyddslag och behörig tillsynsmyndighets utlåtanden och rekommendationer. Parterna är överens om att Biträdesavtalet ska justeras om detta krävs med anledning av Tillämplig dataskyddslag.

4.3 PUB ska säkerställa att samtliga personer som arbetar under dennes ledning följer vad som framgår av Biträdesavtalet och vid var tid gällande instruktion från PUA, samt att de informeras om relevant lagstiftning.

4.4 PUB ska omedelbart underrätta PUA om PUB har otillräckliga eller felaktiga instruktioner avseende PUB:s Behandling av Personuppgifter eller om PUB misstänker eller upptäcker att PUA:s instruktioner strider mot Tillämplig dataskyddslag.

5 SÄKERHET

5.1 PUB ska vid Behandling av Personuppgifter vidta alla lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken och för att skydda Personuppgifter från obehörig eller olaglig behandling, oavsiktlig eller olaglig förlust, förstöring eller ändring eller obehörigt röjande av eller åtkomst till sådana Personuppgifter.

5.2 PUB ska under alla omständigheter vidta sådana tekniska och organisatoriska åtgärder som framgår av *Bilaga 2* till Biträdesavtalet.

6 PERSONUPPGIFTSINCIDENTER

6.1 PUB ska omedelbart underrätta PUA om en misstanke om eller konstaterad personuppgiftsincident som kan leda till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till Personuppgifter. Underrättelsen ska göras till e-postadressen dataskydd@regionhalland.se eller på annat sätt som PUA anvisar.

6.2 PUB ska tillhandahålla PUA följande information avseende personuppgiftsincidenten:

a) en beskrivning av personuppgiftsincidentens art, kategorier av och det ungefärliga antalet Registrerade som berörs, samt de kategorier av och det ungefärliga antalet personuppgiftsposter som berörs,

b) namnet på och kontaktuppgifterna för dataskyddsombudet eller andra kontaktpunkter där mer information kan erhållas,

c) en beskrivning av de sannolika konsekvenserna av personuppgiftsincidenten, samt

d) en beskrivning av de åtgärder som PUB har vidtagit eller föreslagit för att åtgärda personuppgiftsincidenten, inbegripet åtgärder för att mildra dess potentiella negativa effekter.

7 SKYLDIGHET ATT BISTÅ PUA

7.1 PUB ska utan onödigt dröjsmål bistå PUA, i relation till en begäran från Registrerad, om tillgång, rättelse, radering, blockering eller överföring av Personuppgifter, inklusive att tillhandahålla all relevant information och dokumentation, i den mån och utsträckning detta krävs under Tillämplig dataskyddslag. PUB ska inte utföra någon åtgärd med följden att PUA anses handla i strid med Tillämplig dataskyddslag.

7.2 PUB ska, med beaktande av typen av Behandling och den information som PUB har att tillgå, vara skyldig att på PUA:s skriftliga begäran bistå PUA så att denne kan fullgöra de skyldigheter som PUA har avseende säkerhet, personuppgiftsincidenter, konsekvensbedömningar avseende dataskydd och förhandssamråd med behörig tillsynsmyndighet enligt Tillämplig dataskyddslag.

8 SEKRETESS

8.1 PUB och den personal som arbetar under Biträdesavtalet ska iaktta såväl handlingssekretess och tystnadsplikt. Personuppgifter som Behandlas inom ramen för Biträdesavtalet får inte nyttjas eller spridas för andra ändamål, vare sig direkt eller indirekt, om inte PUA skriftligen medgivit detta.

8.2 PUB ska tillse att samtliga anställda, konsulter och övriga som PUB svarar för och som Behandlar Personuppgifter är bundna av en sekretessförbindelse. PUB åtar sig även att tillse att det finns sekretessavtal med eventuella Underbiträden samt sekretessförbindelser mellan Underbiträdet och dess personal.

8.3 PUB:s sekretessåtagande gäller även efter att Biträdesavtalet upphört att gälla, utan begränsning i tid.

9 UTLÄMNANDE AV PERSONUPPGIFTER

9.1 Om Registrerad, behörig tillsynsmyndighet eller annan tredje man begär information från PUB som rör eller kan vara av betydelse för Behandling av Personuppgifter, ska PUB omedelbart skriftligen informera PUA om begäran och innehåll. PUB får inte lämna ut Personuppgifter eller annan information om Behandling av Personuppgifter utan uttrycklig instruktion från PUA, eller om utlämnandet krävs enligt lag.

9.2 PUB ska omedelbart skriftligen underrätta PUA om eventuella kontakter med behörig tillsynsmyndighet avseende Behandling av Personuppgifter. PUB har inte rätt att företräda PUA eller agera för PUA:s räkning gentemot behörig tillsynsmyndighet.

10 UNDERBITRÄDEN

10.1 PUB har rätt att anlita Underbiträde för fullgörandet av PUB:s åtaganden enligt Biträdesavtalet, förutsatt att:

a) PUB informerar PUA om sina avsikter att använda eller byta ut Underbiträde varpå PUA har rätt att göra invändningar mot en sådan förändring, samt

b) Underbiträdet genom ett så kallat underbiträdesavtal med PUB åläggs samma skyldigheter i fråga om dataskydd som de som fastställs i Biträdesavtalet och framför allt att ge tillräckliga garantier om att genomföra lämpliga tekniska och organisatoriska åtgärder på ett sådant sätt att Behandlingen uppfyller kraven i Tillämplig dataskyddslag.

10.2 PUB:s information till PUA enligt punkt 10.1 ovan ska innehålla uppgift om Underbiträdets namn, platsen för Behandlingen samt vilken typ av Behandling Underbiträdet ska utföra för PUB:s räkning. PUA har rätt att begära kopia på ingånget underbiträdesavtal som utan onödigt dröjsmål, dock senast inom trettio (30) dagar, skickas till PUA.

10.3 För det fall att PUA har invänt mot Underbiträde enligt punkt 10.1 ovan ska Parterna tillsammans diskutera möjliga åtgärder för att lösa orsaken till PUA:s invändning. Om Parterna inte kan komma överens om någon lösning inom en rimlig tid, vilket inte ska överstiga trettio (30) dagar, har PUA rätt att säga upp Tjänsteavtalet med PUB genom att meddela detta skriftligen till PUB. PUB ska då återbetala alla eventuella betalningar som gjorts i förskott för de avtalade tjänsterna under Tjänsteavtalet.

10.4 PUA har rätt att återkalla ett godkännande av Underbiträdet om PUA bedömer att Underbiträdet inte efterlever skyldigheterna enligt Biträdesavtalet eller Tillämplig dataskyddslag.

10.5 PUB ska säkerställa att PUA har kännedom om vilka Underbiträden som Behandlar Personuppgifter genom att, på begäran av PUA tillhandahålla PUA fullständig, korrekt och uppdaterad information om samtliga Underbiträden, där följande information specificeras för varje enskilt Underbiträde:

a) definition av Underbiträdet, inklusive dess kontaktinformation, bolagsform och geografisk placering,

b) vilken typ av tjänst som Underbiträdet utför,

c) garantier som uppställs för att kraven i Tillämplig dataskyddslag kommer att följas, samt

d) var Underbiträdet Behandlar Personuppgifter som omfattas av Biträdesavtalet.

10.6 En lista på de Underbiträden som anlitats för Behandling av Personuppgifter framgår av *Bilaga 3* till Biträdesavtalet.

10.7 Om Underbiträdet inte uppfyller sina skyldigheter i fråga om Behandling av Personuppgifter enligt underbiträdesavtalet ska PUB förbli fullt ansvarig gentemot PUA för Underbiträdets uppfyllande av Underbiträdets skyldigheter enligt Biträdesavtalet samt Tillämplig dataskyddslag.

11 TREDJELANDSÖVERFÖRING

11.1 PUB får inte vare sig själv eller genom Underbiträde utan PUA:s skriftliga förhandsgodkännande Behandla Personuppgifter i ett tredje land.

11.2 Om PUB, med PUA:s på förhand lämnade skriftliga godkännande, kommer att Behandla Personuppgifter i tredje land ska PUB dessförinnan:

a) undersöka om detta tredje land ställer en adekvat skyddsnivå för personuppgifter enligt ett beslut meddelat av EU-kommissionen och om så är fallet får Personuppgifter Behandlas i detta tredje land, och om sådant beslut inte föreligger,

b) säkerställa att det finns lämpliga skyddsåtgärder på plats enligt Tillämplig dataskyddslag, t.ex. standardiserade dataskyddsbestämmelser som antagits av EU-kommissionen, som omfattar Behandling av Personuppgifter.

11.3 Om Behandling av Personuppgifter i ett tredje land kräver att särskilt avtal baserat på standardiserade dataskyddsbestämmelser ingås har PUB, oavsett om det är PUB eller Underbiträde som ska ingå avtalet, rätt att teckna sådant avtal för PUA:s räkning.

11.4 PUA har rätt att när som helst återta ett godkännande till tredjelandsöverföring enligt denna punkt 11. I sådant fall ska PUB omedelbart upphöra med Behandlingen av Personuppgifter i tredje land och på PUA:s begäran skriftligen bekräfta detta till PUA.

12 GRANSKNING, TILLSYN OCH REVISION

12.1 PUB ska ge PUA tillgång till all information som krävs för att visa att de skyldigheter som följer av Biträdesavtalet och Tillämplig dataskyddslags krav på personuppgiftsbiträden har fullgjorts samt möjliggöra och bidra till granskningar, inbegripet inspektioner, som genomförs av PUA eller av PUA utsedd revisor.

12.2 PUB ska tillåta de inspektioner som behörig tillsynsmyndighet under Tillämplig dataskyddslag kan kräva för säkerställandet av en korrekt Behandling av Personuppgifter. PUB ska följa av behörig tillsynsmyndighets fattade beslut om åtgärder för att uppfylla Tillämplig dataskyddslag.

12.3 PUB ska säkerställa att PUA tillförsäkras motsvarande rätt till granskning i förhållande till anlitade Underbiträden.

12.4 Rätt till granskning enligt denna punkt 12 får även ske efter det att Behandlingen av Personuppgifter har upphört, om syftet är att tillse att PUB uppfyllt sina åtaganden som har beskrivits i Biträdesavtalet.

13 ERSÄTTNING

13.1 PUB har inte, utöver vad som följer av Tjänsteavtalet, rätt till särskild ersättning för att uppfylla förpliktelser enligt Biträdesavtalet eller Tillämplig dataskyddslag.

14 ANSVAR FÖR SKADA

14.1 PUB ska hålla PUA skadelös avseende sådan skada som uppkommit till följd av Behandling av Personuppgifter i strid med Biträdesavtalet, instruktioner från PUA, myndighetsbeslut eller Tillämplig dataskyddslag.

14.2 PUB ska utan oskäligt dröjsmål informera PUA om sådan skadeståndsprocess inleds som har anknytning till Behandling av Personuppgifter enligt Biträdesavtalet. PUB är skyldig att vidta skäliga åtgärder för att begränsa skadeverkningarna av det inträffade.

15 UPPHÖRANDE AV BEHANDLING

15.1 PUB ska efter upphörande av Biträdesavtalet eller Tjänsteavtalet (beroende på vilket som inträffar först) överlämna Personuppgifter till PUA inom trettio (30) dagar. Sedan PUB har överlämnat Personuppgifter till PUA, ska PUB radera Personuppgifter på ett sådant sätt att de inte kan återskapas, såvida inte lagring av Personuppgifter krävs enligt lag.

16 ÄNDRINGAR AV AVTALET

16.1 Ändringar av och tillägg till Biträdesavtalet eller Tjänsteavtalet ska för att vara bindande vara skriftligen avfattade och behörigen undertecknade av Parterna.

16.2 Denna punkt 16 förhindrar inte att PUA kan ändra eller utfärda ytterligare instruktioner i enlighet med vad som framgår av Biträdesavtalet.

17 ÖVERLÅTELSE

17.1 PUB får inte helt eller delvis överlåta Biträdesavtalet till tredje man utan skriftligt medgivande från PUA.

18 AVTALSTID

18.1 Biträdesavtalet gäller tillsvidare och upphör först när PUB slutat Behandla Personuppgifter för PUA:s räkning.

18.2 PUA äger rätt att säga upp Biträdesavtalet med iakttagande av en uppsägningstid om trettio (30) dagar. Uppsägning ska vara skriftlig.

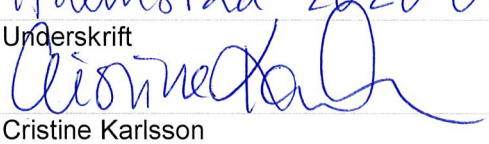
19 TILLÄMPLIG LAG OCH TVIST

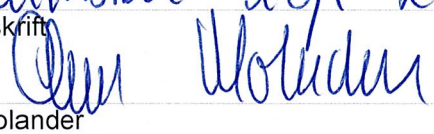
19.1 För Biträdesavtalets tolkning och tillämpning gäller svensk lag.

19.2 Tvist med anledning av Biträdesavtalet ska avgöras enligt vad som överenskommits i Tjänsteavtalet.

Av Biträdesavtalet har åtta (8) originalexemplar upprättats och utväxlats mellan Parterna.

BÄSTA LIVSPLATSEN
Region Halland

Personuppgiftsansvarig **Regionstyrelsen Region Halland**
Ort och datum Halmstad 2020-02-26
Underskrift 
Cristine Karlsson HR-direktör

Personuppgiftsansvarig **Driftnämnden Ambulans, diagnostik och hälsa**
Ort och datum Halmstad 28/1-20
Underskrift 
Ann Molander Ordförande

Personuppgiftsansvarig **Driftnämnden Hallands sjukhus**
Ort och datum Varberg 2020-01-29
Underskrift 
Christian Lidén Ordförande

Personuppgiftsansvarig **Driftnämnden Kultur och skola**
Ort och datum Halmstad 2020-02-11
Underskrift 
Eva Nyhammar Förvaltningschef

BÄSTA LIVSPLATSEN
Region Halland

Personuppgiftsansvarig
Driftnämnden Närsjukvård

Ort och datum
Halmstad 22/2 2020

Underskrift
Margareta Barkström

Margareta Barkström
T f förvaltningschef

Personuppgiftsansvarig
Driftnämnden Psykiatri

Ort och datum
Varberg 2020-02-03

Underskrift

Goran Delic
Förvaltningschef

Personuppgiftsansvarig
Driftnämnden Regionservice

Ort och datum
Halmstad 2020 02 18

Underskrift

Torbjörn Svanberg
Förvaltningschef

Personuppgiftsbiträde
Contica AB

Ort och datum
Göteborg 20191220

Underskrift

Namnförtydligande
Stefan Wånggren
VD

Bilaga 1 - Instruktion vid behandling av personuppgifter

Denna Bilaga 1 till Biträdesavtalet beskriver den Behandling av Personuppgifter som PUB utför för PUA:s räkning under Biträdesavtalet.

Behandlingens föremål

Behandlingens föremål är de personuppgifter som PUB behandlar för PUA:s räkning i samband med fullgörande av Tjänsteavtalet.

Ändamål med behandlingen

PUB behandlar personuppgifter i syfte att tillhandahålla och leverera tjänsterna (IT-konsulting gällande drift, support, utveckling samt tekniskt underhåll av integrationsplattform Biztalk för Region Halland) till PUA och fullgöra sina åtaganden enligt Tjänsteavtalet.

Behandlingens art och omfattning

PUB levererar it-konsulttjänst gällande utveckling, tekniskt underhåll av Region Hallands integrationsplattform Biztalk och drift av densamma på PUA:s uppdrag. PUB kan komma att behandla personuppgifter i samband med att PUB ger support avseende mjukvaran till PUA:s medarbetare. De behandlingssteg som PUB genomför för PUA:s räkning följer av nedanstående tabell och vad som i övrigt framgår av Tjänsteavtalet.

Behandlingssteg	Beskrivning
Åtkomst	PUB kommer åt Personuppgifter i samband med tekniskt underhåll och supportärenden relaterade till mjukvaran.
Insamling	Ej tillämpligt
Överföring och lagring	Ej tillämpligt
Analys	PUB analyserar loggar samt data som kan innehålla Personuppgifter för att söka och åtgärda fel, bistå PUA i supportärenden och genomföra tekniskt underhåll.
Ändring och uppdatering	PUB utvecklar nya och befintliga flöden i Region Hallands integrationsplattform Biztalk för att koppla ihop Region Hallands applikationer på uppdrag av PUA. Dessa flöden används för filöverföringar mellan systemen.

Analys	Filer skickas mellan applikationerna. PUB ändrar eller uppdaterar inte information i filer.
Radering	Vid support använder PUB Region Hallands ärendehanteringssystem för it-ärenden samt eget ärendehanteringssystem. Eventuellt insamlade Personuppgifter och analysresultat (om de innehåller Personuppgifter) raderas efter att supportärendet är avslutat eller när de inte länge behövs för att genomföra tekniskt underhåll. PUB får dock spara de Personuppgifter som är nödvändiga för att dokumentera att supportärendet har genomförts (t.ex. kontaktuppgifter till PUA:s kontaktperson eller kommunikation via e-post) tills Tjänsteavtalet upphör. Sparade Personuppgifter får inte omfatta känsliga Personuppgifter eller patientuppgifter. Om det råder osäkerhet om vilka Personuppgifter som ska sparas ska PUB begära ytterligare skriftliga instruktioner från PUA. I övrigt raderas Personuppgifter enligt PUA:s skriftliga instruktioner.
Administration	PUB hanterar och administrerar Personuppgifter som är nödvändiga för att ge PUA tillgång till tjänsten.

Typ av personuppgifter

Filöverföring innehållande olika slags information sker mellan en mängd olika applikationer. Behandlingen kan omfatta t.ex. namn, personnummer, remissid, anställningsnummer, telefonnummer, e-postadress, övriga kontaktuppgifter och nätidentifierare.

Typ av känsliga personuppgifter

Behandlingen kan omfatta känsliga personuppgifter som hälsa.

Kategorier av registrerade

Behandlingen omfattar PUA:s anställda, konsulter och patienter, samt de kategorier som i övrigt följer av Tjänsteavtalet.

Plats där behandlingen utförs

Behandlingen sker i Region Hallands it-miljö. PUB har åtkomst till denna miljö på distans via egna datorer från PUB:s placering i Göteborg. PUB har egna användarkonton hos Region Halland och använder tvåstegsautentisering för att komma in och arbeta i Region Hallands miljö.

Varaktighet av behandlingen

Behandlingen pågår så länge det är nödvändigt för att tillhandahålla och leverera tjänsterna till PUA och fullgöra sina åtaganden enligt Tjänsteavtalet.

Övriga instruktioner

Inga ytterligare instruktioner är aktuella.

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[1] 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.[2]

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 låsas 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 upplåsning. 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 fjärråtkomst. Behandling av Personuppgifter på mobila enheter ska begränsas enligt dokumenterade rutiner.

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

---

[1] Med it-utrymmen avses samtliga lokaler som är avsedda för it-drift och förvarar it-utrustning.
[2] MSB, 2013, Vägledning för fysisk informationssäkerhet i it-utrymmen, ISBN: 978-91-7383-401-8, tillgänglig på https://www.msb.se/RibData/Filer/pdf/27280.pdf.

Autentisering

Inloggning i system ska ske via personlig användaridentitet 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 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 på 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. Trådlösa 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 finnas 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 finnas 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.[3]

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.

---

[3] Pseudonymisering: behandling av personuppgifter på ett sätt som innebär att personuppgifterna inte längre kan tillskrivas en specifik registrerad utan att kompletterande uppgifter används, under förutsättning att dessa kompletterande uppgifter förvaras separat och är föremål för tekniska och organisatoriska åtgärder som säkerställer att personuppgifterna inte tillskrivs en identifierad eller identifierbar fysisk person.

Bilaga 3 - Underbiträden

Denna Bilaga 3 till Biträdesavtalet anger de Underbiträden som anlitats för Behandling av Personuppgifter under Biträdesavtalet. Förteckningen ska justeras och uppdateras varje gång ett nytt Underbiträde anlitas eller Underbiträde ersätts.

Namn	Org.nr	Typ av tjänst	Plats för behandling