Åbo stads villkor för personuppgiftsbiträden

1 Allmänt

1.1 Denna avtalsbilaga ”Åbo stads villkor för personuppgiftsbiträden” är en del av avtalet om skötseln av en myndighetsuppgift enligt 54 § i kommunallagen, nedan ”Avtalet”.

1.2 I denna avtalsbilaga definieras bindande avtalsvillkor för den ansvariga kommunen och medlemskommunen som rör behandling av personuppgifter och dataskydd, enligt vilka medlemskommunen behandlar personuppgifter för och för den ansvariga kommunens räkning. Om medlemskommunen i samband med att Avtalet genomförs bildar personregister, ansvarar medlemskommunen för dem i egenskap av personuppgiftsansvarig enligt EU:s allmänna dataskyddsförordning.

1.3 Avtalsparterna förbinder sig att i sin verksamhet följa gällande lagstiftning om behandling av personuppgifter och dataskydd, och dessutom förbinder sig Avtalsparterna se till att behandlingen av personuppgifter och dataskyddet följer kravnivån i EU:s allmänna dataskyddsförordning (EU) 2016/679 innan Avtalet börjar verkställas.

2 Avtalsparternas roller i behandlingen av personuppgifter

2.1 Den ansvariga kommunen är personuppgiftsansvarig enligt lagstiftningen om behandling av personuppgifter som ska lagras i arbetskraftsservicens riksomfattande datalager och dataskydd när den fastställer ändamålen och metoderna för behandlingen av personuppgifter. Avtalsparterna förstår att den ansvariga kommunen som personuppgiftsansvarig endast får använda sådana personuppgiftsbiträden som tillgodoser tillräckligt skydd för verkställandet av tekniska och organisatoriska åtgärder så att behandlingen fyller kraven i gällande nationell lagstiftning om behandling av personuppgifter och dataskydd och kraven i EU:s allmänna dataskyddsförordning och att den registrerades rättigheter således säkerställs.

2.2 Medlemskommunen är personuppgiftsbiträde på det sätt som avses i lagstiftningen om behandling av personuppgifter och dataskydd som behandlar den ansvariga kommunens personuppgifter för och för den ansvariga kommunens räkning.

3 Underleverantörer som behandlar personuppgifter

3.1 Medlemskommunen får inte anlita underleverantörstjänster för behandling av personuppgifter utan skriftligt förhandstillstånd från den ansvariga kommunen. Medlemskommunen ska informera den ansvariga kommunen skriftligt om alla planerade ändringar som gäller utökande eller bytande av underleverantörer som är personuppgiftsbiträden. Den ansvariga kommunen har rätt att förbjuda ändringar som medlemskommunen föreslår.

3.2 Till den del som medlemskommunen i sin verksamhet anlitar underleverantörer som behandlar personuppgifter ska utöver Avtalet även villkoren i denna avtalsbilaga tillämpas på underleveranserna. Medlemskommunen är skyldig att genom avtal förbinda de underleverantörer den anlitar att följa villkoren i denna avtalsbilaga.

3.3 Medlemskommunen ansvarar för eventuella överträdelser eller försummelser av Avtalet, denna avtalsbilaga, den tillämpliga lagstiftningen eller EU:s allmänna dataskyddsförordning som en underleverantör som behandlar sysselsättningsområdets personuppgifter gör sig skyldig till som om de vore medlemskommunens egna överträdelser eller försummelser. Om en underleverantör som behandlar personuppgifter inte uppfyller skyldigheterna i anslutning till dataskyddet, är medlemskommunen alltjämt till fullo ansvarig i förhållande till den ansvariga kommunen. Om den ansvariga kommunen av grundad anledning anser att medlemskommunens underleverantör inte uppfyller sina dataskyddsförpliktelser har den ansvariga kommunen rätt att kräva att medlemskommunen byter underleverantör. Medlemskommunen ska på motiverad begäran av den ansvariga kommunen byta underleverantör utan obefogat dröjsmål.

4 Personuppgiftsbiträdets allmänna skyldigheter

4.1 Personuppgiftsbiträdet behandlar personuppgifter i enlighet med lagen och den ansvariga kommunens anvisningar.

4.2 Personuppgiftsbiträdet förbinder sig att säkerställa att alla personer som lyder under det och som har rätt att behandla personuppgifter har förbundit sig att följa sekretess eller att de omfattas av relevant lagstadgad tystnadsplikt.

4.3 Personuppgiftsbiträdet ska också vidta åtgärder för att säkerställa att varje fysisk person som är underställd personuppgiftsbiträdet som har tillgång till personuppgifter endast behandlar dem i enlighet med lag och den ansvariga kommunens anvisningar.

4.4 Personuppgiftsbiträdet förbinder sig till att utan obefogat dröjsmål underrätta den ansvariga kommunen om alla registrerades begäranden som gäller utövande av de registrerades rättigheter enligt gällande lagstiftning och EU:s allmänna dataskyddsförordning.

4.5 Personuppgiftsbiträdet förbinder sig att bistå den ansvariga kommunen med tillbörliga tekniska och organisatoriska åtgärder för att den ansvariga kommunen ska kunna fullgöra sin skyldighet att besvara begäranden som gäller utövande av den registrerades rättigheter. Begäran om utövande av dessa rättigheter kan förutsätta att personuppgiftsbiträdet bistår vid information och kommunikation till den registrerade samt i tillgodoseendet av den registrerades rättigheter.

4.6 Personuppgiftsbiträdet förbinder sig till att vid behov bistå den ansvariga kommunen i att göra en konsekvensbedömning av dataskyddet enligt EU:s allmänna dataskyddsförordning, vid ett eventuellt förhandssamråd och vid anskaffning av en eventuell certifiering av dataskyddet.

4.7 Personuppgiftsbiträdet får inte överföra personuppgifter utanför EU eller EES utan skriftligt förhandstillstånd från den ansvariga kommunen.

4.8 Personuppgiftsbiträdet tillhandahåller den ansvariga kommunen alla uppgifter som behövs för att visa att de skyldigheter som fastställs i denna avtalsbilaga har fullgjorts, och tillåter den ansvariga kommunen att befullmäktiga en revisor att utföra revisioner, inbegripet inspektioner, och deltar också i dem.

5 Personuppgiftsincidenter

5.1 Personuppgiftsbiträdet ska skriftligen underrätta den ansvariga kommunen om personuppgiftsincidenter eller misstänkta personuppgiftsincidenter utan dröjsmål, men senast inom 24 timmar efter delfåendet. Anmälan kan vara preliminär och kan kompletteras efter den utsatta tiden utan obefogat dröjsmål. Den preliminära anmälan ska innehålla följande: 1) vad misstänks ha hänt, när och hur har det kommit fram, 2) preliminär bedömning av vilka personuppgifter och hur många personers uppgifter incidenten gäller och 3) vem ger mer information? Dessutom förbinder sig medlemskommunen att underrätta den ansvariga kommunen om andra väsentliga störningar eller problem som kan ha en inverkan på de registrerades ställning och rättigheter. Anmälan ska göras inom ovan nämnda tidsfrist.

5.2 Personuppgiftsbiträdet ska utan dröjsmål, dock senast inom sju (7) dagar, lämna minst följande uppgifter om personuppgiftsincidenten till den ansvariga kommunen:

1) en beskrivning av personuppgiftsincidenten, inklusive i den mån det är möjligt grupper av relevanta registrerade och uppskattade antal samt grupper av personuppgiftstyper och uppskattade antal;

2) logguppgifter från den tidpunkt då personuppgiftsincidenten inträffade, med vilka avses en i kronologisk ordning registrerad inspelning av händelser i datanät, applikationer, system och datainnehåll och orsakerna till dessa;

3) ange dataskyddsombudet eller någon annan ansvarsperson som kan ge mer information;

4) beskriva de sannolika följderna av personuppgiftsincidenten;

5) lägga fram en bedömning av huruvida personuppgiftsincidenten sannolikt medför en hög risk för den registrerades rättigheter eller friheter; samt

6) beskriva de åtgärder som personuppgiftsbiträdet i fråga föreslår eller har vidtagit på grund av personuppgiftsincidenten och vid behov även åtgärder för att lindra eventuella skadliga verkningar.

6 Övriga krav

6.1 Den ansvariga kommunen har rätt att ändra, komplettera och uppdatera sina anvisningar till medlemskommunen om behandling av personuppgifter och dataskydd. Dessa anvisningar kan vara ändringar, kompletteringar eller uppdateringar av tekniska eller organisatoriska åtgärder som gäller behandling av personuppgifter eller dataskydd. Medlemskommunen och de andra

personuppgiftsbiträdena förbinder sig att iaktta dessa ändrade, kompletterade eller uppdaterade anvisningar.

6.2 Medlemskommunen förbinder sig att reagera senast inom 36 timmar från att den ansvariga kommunen tagit kontakt och att svara senast inom en (1) vecka från den ansvariga kommunens anmälningar, reklamationer eller andra meddelanden som gäller dataskyddet, bortsett från personuppgiftsincidenter enligt EU:s allmänna dataskyddsförordning, på vilka tillämpas de tidsfrister som fastställts i Avtalet och ovan i denna bilaga.

6.3 Om en Avtalspart försummar eller bryter mot denna avtalsbilaga, den tillämpliga lagstiftningen eller EU:s allmänna dataskyddsförordning, bestäms Avtalspartens ersättningsskyldighet förutom Avtalet enligt tillämplig lagstiftning. Dessutom utgör en sådan försummelse eller överträdelse ett väsentligt avtalsbrott som avses i Avtalet, med påföljden att den ansvariga kommunen har rätt att hänvisa till de rättsmedel som fastställts i Avtalet. En mindre försummelse eller överträdelse betraktas inte som ett väsentligt avtalsbrott.

Del II: Beskrivning av behandlingen av personuppgifterna

Avtalsparterna har kommit överens om att Leverantören på Beställarens vägnar behandlar följande personuppgifter för att genomföra den tjänst som avtalas i Avtalet:

Typer av personuppgifter (välj en enligt den största risken):

☐ Låg risk
(t.ex. behandlingen av personuppgifter gäller vanliga kontaktuppgifter)

☐ Medelhög risk
(t.ex. behandlingen av personuppgifter gäller identifierande uppgifter eller exakta kontaktuppgifter)

x Hög risk
(t.ex. behandlingen av personuppgifter gäller känsliga uppgifter, exakta lokaliseringsuppgifter eller exakta identifierande uppgifter)

Personuppgiftsgrupper (välj en enligt den känsligaste personuppgiften):

☐ Sedvanliga personuppgifter

x Särskilda, s.k. känsliga personuppgifter
(ras eller etniskt ursprung, politisk åsikt, religiös eller filosofisk övertygelse eller medlemskap i ett fackförbund samt behandling av genetiska eller biometriska uppgifter för entydig identifiering av en person eller behandling av hälsouppgifter eller uppgifter om en fysisk persons sexuella beteende och läggning)

Längden på behandlingen av personuppgifter (välj en):

x Under avtalets giltighet

☐ Annan tid (dd.mm.åååå–dd.mm.åååå): _____

Typ och syfte med behandlingen av personuppgifter

Medlemskommunen behandlar personuppgifter endast i den omfattning som Avtalet förutsätter.