Handläggare
Kommunstyrelseförvaltningen
Alice Berg
Kommunsekreterare
08-578 28 329
Alice.berg@tyreso.se

Handlingstyp
Beslut

Sida
1 (2)

Datum
2024-02-15

Diarienummer
2024/KS 0027

Mottagare
Storsthlm

Ordförandebeslut om datadelningsavtal för den regionala Energi- och klimatrådgivningen i Stockholms län

Beslut

1. Datadelningsavtal för den regionala Energi- och klimatrådgivningen i Stockholms län (EKR) godkänns.
2. Kommundirektören får i uppdrag att säkerställa verkställandet av de av datadelningsavtalet angivna åtaganden som åläggs varje part som ansvarar för EKR.

Beslutsdatum 2024-02-15

Anita Mattsson
Kommunstyrelsens ordförande

Beslut fattat enligt 6 kap. 39 § Kommunallagen och delegat enligt kommunstyrelsens delegationsordning 2023-12-05 § 162, punkt 1.10

Beskrivning av ärendet

Den regionala Energi- och klimatrådgivningen i Stockholms län (EKR) har analyserat samarbetet utifrån ett GDPR-perspektiv. Den analys som arbetsgruppen med anledning av detta har gjort, har landat i att det inte går att betrakta EKR-samarbetets organisation som en självständigt personuppgiftsansvarig i GDPR:s mening, utan att personuppgiftsansvaret i dataskyddsrättsligt hänseende måste ses som ett s.k. gemensamt personuppgiftsansvar mellan de 26 deltagande kommunernas ansvariga nämnder. I normalfallet innebär detta att varje kommun är fullt ut ansvarig för

all personuppgiftsbehandling som utförs inom ramen för EKR-samverkan. För att klargöra villkoren och förutsättningarna för detta har bifogat avtal tagits fram. Avtalet har tidigare skickats ut för översyn till de kommuner som deltar i EKR-samarbetet.

Ett centralt ställningstagande som GDPR-analysen utmynnade i är att de lagliga grunderna för den personuppgiftsbehandling som sker inom ramen för samarbetet, framför allt är två stycken. Antingen allmänt intresse grundande sig i det allmännas skyldighet att bidra till en god miljö som framgår av 1 kap. 2 § regeringsformen och kommunernas övergripande ansvar för miljökvalitet som framgår av miljöbalken (1998:808), eller rättslig förpliktelse utifrån offentlighetsprincipens skyldighet att hantera och bevara handlingar och uppgifter som inkommer till myndigheter, vilken framgår framför allt av tryckfrihetsförordningen, offentlighets- och sekretesslagen (2009:400), arkivlagen (1990:782) och förvaltningslagen (2017:900).

Som en konsekvens av det gemensamma personuppgiftsansvaret måste var och en av de deltagande kommunerna se till att den personuppgiftsbehandling som sker som en konsekvens av EKR-samarbetet också syns i registerförteckningen (artikel 30-registret) för den kommunala nämnd som deltar i EKR. Beslutet har inga ekonomiska konsekvenser.

Handlingar som ingår i beslutet

Datadelningsavtal EKR

Följebrev till datadelningsavtal EKR

Delges

Storsthlm

Kommunstyrelsen

STORSTHLM

Bifogat till detta brev hittar ni ett datadelningsavtal för den regionala Energi- och klimatrådgivningen i Stockholms län.

Dokumentet har tagits fram av dataskyddsombuden i Stockholm och Huddinge i samarbete med huvudprojektledaren för EKR-samarbetet och har sin upprinnelse i att vi i samband med en personuppgiftsincident våren 2021 insåg att Stockholmsregionens EKR-samarbete inte hade analyserats utifrån ett GDPR-perspektiv. Den analys som arbetsgruppen med anledning av detta har gjort, har landat i att det inte går att betrakta EKR-samarbetets organisation som en självständigt personuppgiftsansvarig i GDPR:s mening, utan att personuppgiftsansvaret i dataskyddsrättsligt hänseende måste ses som ett s.k. gemensamt personuppgiftsansvar mellan de 26 deltagande kommunernas ansvariga nämnder. I normalfallet innebär detta att varje kommun är fullt ut ansvarig för all personuppgiftsbehandling som utförs inom ramen för EKR-samverkan. För att klargöra villkoren och förutsättningarna för detta har bifogat avtal tagits fram. Avtalet har tidigare skickats ut för översyn till de kommuner som deltar i EKR-samarbetet och den version ni nu får har beaktat de synpunkter som då inkom.

Ett centralt ställningstagande som GDPR-analysen utmynnade i är att de lagliga grunderna för den personuppgiftsbehandling som sker inom ramen för samarbetet, framför allt är två stycken. Antingen **allmänt intresse** grundande sig i det allmännas skyldighet att bidra till en god miljö som framgår av 1 kap. 2 § regeringsformen och kommunernas övergripande ansvar för miljökvalitet som framgår av miljöbalken (1998:808), eller **rättslig förpliktelse** utifrån offentlighetsprincipens skyldighet att hantera och bevara handlingar och uppgifter som inkommer till myndigheter, vilken framgår framför allt av tryckfrihetsförordningen, offentlighets- och sekretesslagen (2009:400), arkivlagen (1990:782) och förvaltningslagen (2017:900).

Som en konsekvens av det gemensamma personuppgiftsansvaret måste var och en av de deltagande kommunerna se till att den personuppgiftsbehandling som sker som en konsekvens av EKR-samarbetet också syns i registerförteckningen (artikel 30-registret) för den kommunala nämnd som deltar i EKR.

Om ni har några frågor är ni välkomna att höra av er till Malin Lindstaf
malin.lindstaf@stockholm.se

Med vänlig hälsning

Värdkommunerna för Samarbetet Energi-och klimatrådgivningen i Stockholms län

STORSTHLM

2023-10-24
S/23/0131

DATADELNINGSAVTAL

Gällande personuppgiftsbehandling inom ramen för regionala Energi- och klimatrådgivningen i Stockholms län

INNEHÅLLSFÖRTECKNING

BILAGOR

Detta **DATADELNINGSAVTAL** har träffats mellan:

(1) Botkyrka kommun, 212000-2882, 147 85 Tumba

(2) Danderyds kommun, 212000-0126, Tekniska kontoret Mörbygårdsvägen 4, 5 tr 182 31 Danderyd

(3) Ekerö kommun, 212000-0050, Tappströmsv 2 178 32 Ekerö

(4) Haninge kommun, 212000-0084, Rudsjöterrassen 2 136 81 Haninge

(5) Huddinge kommun, 212000-0068, Miljö & Bygglovsförvaltningen Hälsovägen 7 141 57 Huddinge

(6) Järfälla kommun, 212000-0043, Kommunstyrelseförvaltningen Vasaplatsen 11, 3 tr 177 57 Järfälla

(7) Lidingö stad, 212000-0191, Miljö- och stadsbyggnadskontoret Lejonvägen 15 181 82 Lidingö

(8) Nacka kommun, 212000-0167, Granitvägen 15 131 81 Nacka

(9) Norrtälje kommun, 212000-0217, Estunavägen 14 Box 800 761 28 Norrtälje

(10) Nykvarns kommun, 212000-2999, Centrumvägen 26 155 80 Nykvarn

(11) Nynäshamns kommun, 212000-0233, Stadshusplatsen 1 149 81 Nynäshamn

(12) Salems kommun, 212000-2874, Säby torg 16 144 80 Rönninge

(13) Sigtuna kommun, 212000-0225, Södergatan 20 195 85 Märsta

(14) Sollentuna kommun, 212 000-0134, Norra Malmvägen 143 191 86 Sollentuna

(15) Solna stad, 212000-0183, Miljö- och byggnadsförvaltningen Stadshusgången 2 17186 Solna

(16) Stockholms stad, 212000-0142, Miljöförvaltningen, enhet Energi och Klimat Pipersg. 34 112 28 Stockholm

(17) Sundbybergs stad, 212000-0175, Östra Madenvägen 4 172 92 Sundbyberg

(18) Södertälje kommun, 212000-0159, Nyköpingsv. 26 151 89 Södertälje

(19) Tyresö kommun, 212000-0092, Dalgränd 6, 135 40 Tyresö

(20) Täby kommun, 212000-0118, Attundavägen 22-24 183 34 Täby

(21) Upplands Väsby kommun, 212000-0019, Dragonvägen 86 194 80 Upplands Väsby

(22) Upplands-Bro kommun, 212000-0100, Tillväxtkontoret 196 81 Kungsängen

(23) Vallentuna kommun, 212000-0027, Kommunledningskontoret 186 86 Vallentuna

(24) Vaxholms stad, 212000-2908, Eriksöv. 27 185 83 Vaxholm

(25) Värmdö kommun, 212000-0035, Skogsbovägen 9-11 134 81 Gustavsberg

(26) Österåkers kommun, 212000-2890, Samhällsbyggnadsförvaltningen Hackstavägen 22 184 86 Åkersberga

”**Parterna** till detta Datadelningsavtal är ovanstående parter, tillsammans benämnda Parterna och var för sig Part.”

Dessa, samt övriga definitioner, ska tolkas i enlighet med avsnitt 1 nedan i detta Avtal.

BAKGRUND

A. Syftet med detta datadelningsavtal (”Datadelningsavtalet”) är att tydliggöra ansvarsfördelningen mellan Parterna, avseende behandling av personuppgifter mellan Parterna. Datadelningsavtalet ska reglera de inbördes arrangemangen för behandling av personuppgifter mellan Parterna. Datadelningsavtalet ska vidare säkerställa att de registrerades rättigheter omhändertas enligt artikel 26 i enlighet med gällande dataskyddslagstiftning.

B. Datadelningsavtalet fastställer Parternas gemensamma personuppgiftsansvar.

C. Datadelningsavtalet avser personuppgiftsbehandling inom den gemensamma Energi- och klimatrådgivningen i Stockholms län. Enligt den samverkansöverenskommelse som reglerar samarbetet inom Energi- och klimatrådgivningen ska den i överenskommelsen reglerade styrgruppen fastställa årliga inriktningsbeslut och årlig verksamhetsplan för samarbetet med utgångspunkt i de samverkande parternas prioriteringar och de av staten angivna förutsättningarna för statsbidraget. Av den av parterna gemensamt antagna verksamhetsbeskrivningen framgår att styrgruppen ansvarar för verksamhetens operativa arbete och bl.a. ska fastställa riktlinjer för GDPR. Styrgruppen är ett gemensamt beslutsorgan för de i samverkansöverenskommelsen ingående parterna och då styrgruppen fastställer ändamål och medel för behandlingen av personuppgifter i verksamheten har de i samverkansöverenskommelsen ingående parterna ett gemensamt personuppgiftsansvar.

D. För att garantera en säker, korrekt och laglig behandling av personuppgifterna i samband med genomförandet av Uppdraget och för att fastställa Parternas respektive skyldigheter för behandlingen av personuppgifter har Parterna kommit överens om att ingå detta Datadelningsavtal på de villkor som anges nedan.

1. DEFINITIONER OCH TOLKNING

1.1 DEFINITIONER

”**Dataskyddsförordningen**” avser 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 upphävandet av direktiv 95/46/EG (allmän dataskyddsförordning) inklusive alla eventuella ändringar i Dataskyddsförordningen.

”**EU-reglering**” avser från och med den 25 maj 2018 Dataskyddsförordningen.

”**Gällande Rätt**” avser all den lagstiftning som är tillämplig på behandlingen av personuppgifter, inklusive EU-regleringen, sådan lagstiftning som vid varje tidpunkt kan ersätta ovan nämnd lagstiftning (för det fall skillnader eller motsägelser förekommer mellan olika bestämmelser eller regler så ska den bestämmelse som medför det starkaste integritets- och/eller informationsskyddet tillämpas).

”**Huvudavtalet**” avser alla dokument där parterna reglerar vad som ingår i Uppdraget och hur det ska utföras.

”**Part**” och ”**Parterna**” avser ovanstående parter, var för sig eller gemensamt, beroende på situationen och som den beskrivs i Huvudavtalet.

”Energirådgivningen” avser regionala Energi- och klimatrådgivningen i Stockholms län.

”Storsthlm” avser kommunförbundet Storsthlm.

”**Tillsynsmyndighet**” avser varje domstol, myndighet eller organ som enligt tillämplig lagstiftning och/eller förordning (inklusive Gällande Rätt), utövar tillsyn över integritetsfrågor och/eller behandling av personuppgifter.

“**Uppdraget**” avser den behandling av personuppgifter parterna är gemensamt personuppgiftsansvariga som det beskrivs i punkt C ovan samt i bilaga 1.

1.2 **TOLKNING**

1.2.1 Begrepp och uttryck i detta Datadelningsavtal som inte inleds med versal, t.ex. ”registrerad”, ”personuppgiftsansvarig”, ”personuppgift”, ”behandling”, ”personuppgiftsbiträde”, ”tredje land” etc., ska ha den innebörd som dessa ges i EU-regleringen.

1.2.2 Om inte annat uttryckligen framgår av detta Datadelningsavtal, eller tydligt framgår av den kontext i vilken begreppet används, ska begreppet ”inklusive” innebära ”inklusive utan att vara begränsat till”.

2. AVTALETS OMFATTNING

2.1 Parterna fastställer ändamål och medel för behandlingen av personuppgifter i enlighet med avsnittet Bakgrund och punkten C ovan och i enlighet med vad som närmare beskrivs i ”Beskrivningen av behandling av personuppgifter” (Bilaga 1), där omfattningen av personuppgiftsbehandlingen framgår. Detta avtal utgör Parternas arrangemang för gemensamt personuppgiftsansvar enligt artikel 26 Dataskyddsförordningen.

2.2 Parterna är vidare överens om att vardera Part är ensamt personuppgiftsansvarig för all personuppgiftsbehandling som sker utanför ramen för Uppdraget eller när Uppdraget är avslutat.

3. PARTERNAS ÅTAGANDEN

3.1 De Personuppgiftsansvariga Parterna ansvarar för behandling av avtalade personuppgifter i enlighet med Dataskyddsförordningen/GDPR.

3.2 Parterna åtar sig att tillse att den personuppgiftsbehandling som sker under Huvudavtalet utförs i enlighet med detta Datadelningsavtal och Gällande rätt.

3.3 Parterna ska säkerställa att personuppgifter behandlas konfidentiellt vilket bland annat innebär att endast de anställda, konsulter och Underbiträden som behöver tillgång till personuppgifterna för att utföra Uppdraget har tillgång till personuppgifterna samt att de som får tillgång till personuppgifterna iakttar sekretess i förhållande till personuppgifterna.

3.4 Parterna ska skydda de personuppgifter som behandlas och vidta lämpliga åtgärder för att säkerställa en säkerhetsnivå som i enlighet med parternas skriftliga överenskommelser är lämplig i förhållande till risken. Parterna ska även skydda de personuppgifter som behandlas från obehörig eller olaglig behandling, oavsiktlig eller olaglig förlust, förstöring eller ändring eller obehörigt röjande av eller åtkomst till sådana personuppgifter. Om personuppgifterna som behandlas är känsliga ska Parterna vidta eventuella ytterligare sådana åtgärder som är lämpliga för skydd av dessa.

3.5 Varje Part ska svara för att upprätta och vidmakthålla nödvändig dokumentation om sina respektive personuppgiftsbehandlingar och hålla övriga parter informerade om behandlingarna. Part ska utan dröjsmål rapportera viktigare händelser till Storsthlm som svarar för att informationen kommer övriga parter och styrgruppen för Energirådgivningen till del.

3.6 Om en Part tar emot en begäran från en registrerad om tillgång till personuppgifter, dataportabilitet, rättelse, radering, begränsning eller invändning av behandling av personuppgifter ska de andra Parterna informeras. Parterna åtar sig att tillhandahålla varandra erforderligt stöd för fullgörande av sådan begäran i enlighet med Gällande Rätt.

3.7 Varje Part ska omedelbart informera Storsthlm och de andra Parterna om en misstanke om eller konstaterat a) brott mot detta Datadelningsavtal, och b) personuppgiftsincident i relation till personuppgifterna som behandlas i samband med Uppdraget. Det är respektive Part där incidenten inträffar som ansvarar för att hantering av personuppgiftsincidenter fullgörs i enlighet med Gällande rätt. Den Part där incidenten inträffar ska assistera övriga berörda Parter i framtagandet av information och rapporter till registrerade och myndigheter. Alla berörda Parter ska, i den mån det är möjligt, vidta rimliga åtgärder för att begränsa skada som en registrerad har lidit. De Parter som berörts av incidenten ska även dokumentera dessa i enlighet med gällande rätt och ska, i tillägg till ovan, samarbeta med andra berörda avtalsparter för att säkerställa att gällande rätt efterlevs och tillämpas. Värdkommunerna har, i den utsträckning dessa berörs av incidenten, ett särskilt ansvar för att incidenten rapporteras till IMY och även att drabbade registrerade ges information, i de fall detta ska göras. Värdkommunerna ansvarar även för att övriga samverkanskommuner samt Storsthlm får sammanfattande information om det inträffade.

3.8 En särskild statusrapport om personuppgiftsbehandlingarna inom ramen för partssamarbetet ska lämnas årligen, senast den 31 december till Storsthlm för föredragning för styrgruppen och vid behov information till övriga parter.

4. UNDERBITRÄDEN

4.1 Ingen av Parterna har rätt att anlita Underleverantörer för behandling av personuppgifter inom Uppdraget utan att först inhämta skriftliga godkännanden från andra berörda parter.

4.2 Anlitas Underbiträde efter godkännande enligt föregående punkt, ska utförande part svara för Underbiträdets utförda arbete som om denne själv utfört arbetet enligt Datadelningsavtalet.

5. SÄKERHETSÅTGÄRDER

5.1 Varje Part ska, med hänsyn till behandlingens art, vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken som beskrivs i artikel 32 Dataskyddsförordningen, såsom kryptering av personuppgifter och säkerställandet av konfidentialitet och integritet i förhållande till system och tjänster som används vid behandling av personuppgifter.

5.2 Parterna ska, enskilt eller gemensamt, upprätta instruktioner och riktlinjer för de säkerhetsåtgärder som ska vidtas. Säkerhetsåtgärderna som ska vidtas framgår av Bilaga 2 om inte Parterna kommit överens om att dokumentera säkerhetsåtgärderna på annan plats. Utöver de säkerhetsåtgärder som vidtas ska instruktionerna även innehålla övervakning av skyddsåtgärdernas efterlevnad och tillämpning.

6. AVTALSTID OCH UPPSÄGNING

Detta Datadelningsavtal gäller från och med att det godkänt av samtliga Parter och undertecknats av respektive parts representant. Avtalet gäller till dess att samarbetet har upphört., varvid detta Datadelningsavtal ska upphöra att gälla automatiskt utan ytterligare uppsägningstid. Vid uppsägning av Datadelningsavtalet ska Part utan onödigt dröjsmål framställa tydlig begäran till berörda Parter om att dessa överlämnar samtliga Personuppgifter till den begärande Part, eller raderar dem i enlighet med begärande Parts

önskemål. Om Personuppgifterna överlämnas ska det ske i ett öppet och standardiserat format. Med samtliga Personuppgifter avses alla Personuppgifter vilka har omfattats av Behandlingen samt annan tillhörande information såsom Loggar, Instruktioner, systemlösningar, beskrivningar och andra handlingar som Personuppgiftsbiträdet erhållit genom informationsutbyte enligt Datadelningsavtalet.

Part får som längst fortsätta med behandling av personuppgifterna i enlighet med Datadelningsavtalet och övriga partsöverenskommelser under ytterligare maximalt tre månader efter Datadelningsavtalets upphörande.

7. ANSVAR

7.1 Parterna erkänner att den registrerade har rätt att utöva sina rättigheter i förhållande till alla Parter och att varje Part är fullt ansvarig i förhållande till den registrerade för den skada som uppkommit i samband med behandling av personuppgifter enligt detta Datadelningsavtal, såvida Parten i fråga inte kan styrka att den inte på något sätt orsakat skadan.

7.2 Vardera Part ska hålla de andra Parterna skadeslösa för samtliga skador i händelse av anspråk från tredje man på grund av, som uppstår ur eller som har samband med förstnämnda Partens avtalsbrott.

8. TILLÄMPLIG LAG OCH TVISTER

8.1 Parternas rättigheter och skyldigheter enligt detta avtal bestäms i sin helhet av svensk rätt.

8.2 Tvist angående tolkning eller tillämpning av detta avtal ska avgöras enligt svensk lag och föras vid allmän svensk domstol.

Detta Avtal har upprättats i 26 likalydande exemplar varav parterna tagit var sitt.

Ort
Datum

Organisationens namn

_____

Signatur

_____

BILAGA 1

BESKRIVNING AV BEHANDLINGEN AV PERSONUPPGIFTER

1. UPPDRAGET

Utförandet av Uppdraget kommer att innebära behandling av personuppgifter som denna bilaga avser att beskriva närmare. Uppdraget avser den gemensamma Energirådgivningen i Stockholms län. Verksamheten i Energirådgivningen bedrivs i huvudsak i projektform men har också mer permanenta inslag såsom drift av hemsida och rådgivning via telefon, e-post och videomöten. Energirådgivningen riktar sig till hushåll och privatpersoner, företag, föreningar och andra organisationer i de samverkande kommunerna. Energirådgivningen har ett gemensamt telefonnummer och en gemensam e-postadress. Till följd av den här konstruktionen behandlas personuppgifter i olika delar av detta partssamarbete av en viss Part för samtliga samverkande Parters räkning.

2. ÄNDAMÅL BEHANDLINGEN AV PERSONUPPGIFTER

Ändamålet med behandlingen av personuppgifter är att ge hushåll och privatpersoner, företag, föreningar och andra organisationer i de samverkande kommunerna rådgivning inom energi- och klimatfrågor.

3. LAGLIG GRUND FÖR BEHANDLINGEN AV PERSONUPPGIFTER

Den lagliga grunden för behandlingen av personuppgifter är för att fullgöra en uppgift av allmänt intresse och för att fullgöra rättsliga förpliktelser.

Med *uppgift av allmänt intresse* avses det allmännas skyldighet till att bidra till en god miljö (1 kap. 2 § Regeringsformen). Kommunal energi- och klimatrådgivning är ett led i detta (jfr. 5-6 §§ förordning [2016:385] om bidrag till kommunal energi- och klimatrådgivning och prop. 1996/97:84, avsnitt 7.4.5).

Med *rättsliga förpliktelser* avses de skyldigheter som åligger Parterna i egenskap av kommuner enligt lag, framförallt förvaltningslagen (2017:900), kommunallagen (2017:725), arkivlagen (1990:782) och offentlighets- och sekretesslagen (2009:400).

4. KATEGORIER AV PERSONUPPGIFTER

Behandlingen av personuppgifter inom Uppdraget kommer framför allt att omfatta följande kategorier av personuppgifter:

- Kontaktuppgifter, namn, mejladress, telefonnummer- till berörda tjänstepersoner hos de samverkande parterna.
- Namn, mejladress, telefonnummer samt kommuntillhörighet till personer som kontaktar den gemensamma telefon- och mejlrådgivningen
- Namn och mejladress samt kommuntillhörighet till deltagare i seminarier.
- Namn och mejladress till leverantörer.
- Namn och mejladress samt telefonnummer till deltagare i Energirådgivningens projekt.
- I förekommande fall fotografier av deltagare i projekt.
- Ljudupptagning av presentationer (tjänstepersoner).

5. PERSONUPPGIFTSBEHANDLINGENS VARAKTIGHET

Vardera Part behandlar personuppgifterna i enlighet med Gällande rätt, i enlighet med parternas gemensamma överenskommelser och i enlighet med respektive parts Informationshanteringspolicy/dokumenthanteringspolicy och gallringsinstruktioner.

6. SÄKERHETSÅTGÄRDER

Varje Part ska i enlighet med avsnitt 5 i Avtalet uppfylla de krav på säkerhetsåtgärder som följer av Bilaga 2 Tekniska och organisatoriska säkerhetsåtgärder, som bifogats detta Datadelningsavtal.

BILAGA 2

TEKNISKA OCH ORGANISATORISKA SÄKERHETSÅTGÄRDER

Bakgrund och syfte

Den speciella situationen med delvis gemensamt personuppgiftsansvar mellan parterna ställer särskilda krav på säkerhet. Särskilda säkerhetsåtgärder måste t.ex. vidtas för att skydda sådan information som behandlas i verksamheten och som omfattas av sekretess eller krav på säkerhetsskydd enligt lag.

För den som är personuppgiftsansvarig, gemensamt eller självständigt i förhållande till de andra Parterna inom ramen för Datadelningsavtalet, är det nödvändigt att tillse att denne tillhörig information ej obehörigen röjs, ändras, görs otillgänglig för behöriga eller förstörs. Syftet med bilagan är att tillse att Datadelningsavtalet fullgörs på ett sådant sätt som tillgodoser Parternas behov av informationssäkerhet. De tekniska och organisatoriska säkerhetsåtgärder som Parterna i Datadelningsavtalet åtar sig att fullgöra ska säkerställa upprätthållande av konfidentialitet, tillgänglighet, riktighet och spårbarhet med avseende på den information som de personuppgiftsansvariga ansvarar för.

De personuppgiftsansvarigas information ska skyddas från oavsiktlig eller otillåten förlust, förstörelse, ändring och tillgängliggörande för obehöriga.

Åtkomstskydd

Det ska säkerställas att inloggning i system hos vardera Part endast omfattar den del i systemet som krävs för de behandlingar som avtalats. Om uppgifter tas ut från system/databas ska datorutrustning och löstagbara datamedier hos Parten, låsas in för att skyddas mot obehörig användning, påverkan eller stöld, när det inte hålles under uppsikt. I annat fall ska personuppgifterna krypteras. Om bärbara datorer används vid behandlingar ska personuppgifterna på fasta och löstagbara lagringsmedier vara krypterade. Vid systemarbeten utförda på distans ska kommunikationen skyddas av VPN-teknik.

Behörighetskontroll

Ett tekniskt system för behörighetskontroll ska styra åtkomsten till personuppgifterna hos Part. Behörigheten ska begränsas till den enhet som avses samt till dem som behöver uppgifterna för sitt arbete. Användaridentitet och lösenord ska vara personliga och får inte överlåtas eller utlånas till annan. Det ska finnas rutiner för tilldelning och borttagande av behörigheter. Extra kontroll av behörigheter ska ske vid förändring i personalen.

Säkerhetskopia

Personuppgifterna ska regelbundet överföras till krypterade säkerhetskopior i vardera Parts system. Kopiorna ska förvaras avskilt och väl skyddade så att personuppgifterna kan återskapas efter en störning. Utförande Part ska ha en rutin för test av återläsning.

Datakommunikation

Anslutning för extern datakommunikation ska skyddas med sådan teknisk funktion som säkerställer att uppkopplingen är behörig. Personuppgifter som överförs via datorkommunikation utanför lokaler som kontrolleras av Parten ska skyddas med kryptering eller annan säker metod.

Personuppgiftsincidenter

Incidenter hänförliga till det gemensamma personuppgiftsansvaret ska utan dröjsmål rapporteras till alla Parter i avtalet och innehålla redogörelse för vad som har hänt och vilka åtgärder Part vidtagit med anledning av Incidenten. Parterna ska ha lämpliga rutiner för att genomföra, rapportera och följa upp Incidentutredningar. Behörighet att utföra Incidentutredningar enligt detta avtal ska hos vardera Parten vara begränsat till ett fåtal personer.

Övriga Tekniska och organisatoriska säkerhetsåtgärder

Part ska säkerställa att erforderligt skydd mot skadlig kod upprätthålls för de delar av Uppdraget som denne ansvarar för.

Det ska ske genom att ny information kontrolleras innan den tillförs IT-system som används för Uppdragets genomförande i syfte att säkerställa att information innehållande skadlig kod ej tillförs. Programvara som skyddar mot skadlig kod ska uppdateras kontinuerligt enligt Parts riktlinjer för skydd mot skadlig kod, vilka ska kunna visas för övriga Parter.

IT-system som används för genomförande av Uppdraget ska skyddas mot externa angrepp av brandväggar. IT-system som används för genomförande av Uppdraget ska ha skydd mot intrång och möjliggöra intrångsdetektering. Parts riktlinjer för intrångsdetektering och skydd mot intrång ska dokumenteras av Part och vid förfrågan kunna visas för övriga Parter.

All kommunikation vid inloggningsförfarandet, sessionskommunikation och integrationsöverföring ska vara krypterad med för ändamålet adekvat säkerhetsnivå. Part utser en reservrutin som kan användas om dess IT-system är ur funktion och det stör Uppdragets genomförande i väsentlig omfattning. Part ska dokumentera vilken reservrutin som ska användas för det fall IT-systemet ligger nere i sådan omfattning att det stör genomförandet av Uppdraget.

Part ska fortlöpande testa system eller databaser som används för dennes fullgörande av Uppdraget avseende attacker och intrång. I samband med sådana tester ska löpande integritetskontroll ske. Detta gäller även system eller databaser som ska tillhandahållas inom Uppdraget. Part ska i rimlig omfattning genomföra proaktiva säkerhetstester av tjänster som Part ska tillhandahålla inom Uppdraget.

BILAGA 3

CHECKLISTA FÖR UNDERRÄTTELSE

1. INFORMATION TILL DE REGISTRERADE

Respektive Part ska ge följande information till den registrerade:

1. Identitet och kontaktuppgifter för de gemensamt personuppgiftsansvariga;

2. Ändamålen med den behandling för vilken personuppgifterna är avsedda;

3. Den lagliga grunden för behandlingen (t.ex. fullgörande av avtal, allmänt intresse eller rättslig förpliktelse);

4. De kategorier av personuppgifter som behandlas (om uppgifter inhämtas från andra källor än individen, specificera varifrån uppgifterna hämtats och huruvida uppgifterna härrör från allmänt tillgängliga källor);

5. Mottagarna eller de kategorier av mottagare som ska ta del av personuppgifterna;

6. I tillämpliga fall att den personuppgiftsansvarige avser att överföra personuppgifter till ett tredjeland och huruvida adekvat skyddsnivå föreligger eller saknas (t.ex. EU:s standardavtalsklausuler);

7. Information om att Beställaren kommer att spara individens personuppgifter för tillgodoseende av offentlighetsprincipen och arkivlagens bestämmelser;

8. Den period under vilken personuppgifterna kommer att lagras (eller de kriterier som används för att fastställa denna period);

9. Att det, med de begränsningar som följer av punkt 7, föreligger en rätt för individen att begära tillgång till och rättelse eller radering av dennes personuppgifter;

10. Att det föreligger en rätt för individen att begära en begränsning av behandling eller att invända mot behandling samt rätten till dataportabilitet;

11. Rätten att inge klagomål till en tillsynsmyndighet;

12. Den eventuella förekomsten av automatiserat beslutsfattande (inbegripen profilering), logiken bakom samt betydelsen och de förutsedda följderna av sådan behandling.