Gemensamt personuppgiftsansvar i det webbaserade informationssystemet WIS

1. Bakgrund och syfte

WIS är en portal för Sveriges krisberedskap som underlättar för aktörer att dela information före, under och efter samhällsstörningar. I WIS delas information baserat på ytor. Användare kan följa ytor av intresse eller aktivt publicera information. Informationen kan vara anteckningar, lägesrapporter, dokument och enkla kartnoteringar. Aktörer kan vid behov begära in information från övriga aktörer. För att vara säker på att inte missa nya händelser kan användare välja att bevaka ämnen eller geografiska områden som intresserar dem och sen välja att få aviseringar om detta.

Varje aktör i WIS äger sin egen information och väljer själv vilka man vill dela den med. Det går även att använda WIS för att dela information enbart inom egen organisation. För WIS finns administrativa bestämmelser som alla aktörer i WIS måste följa.

Denna handling utgör ett sådant arrangemang om gemensamt personuppgiftsansvar som följer av dataskyddsförordningens (GDPR:s) artikel 26. Arrangemanget återspeglar de gemensamt personuppgiftsansvarigas respektive roller och förhållanden gentemot registrerade i det webbaserade informationssystemet WIS.

Dåvarande Krisberedskapsmyndigheten, KBM, fick under 2004 i uppdrag av regeringen att utveckla WIS. När MSB etablerades den 1 januari 2009 fördes uppdraget att utveckla och förvalta WIS vidare till den nya myndigheten.

Den registrerade får alltid utöva sina rättigheter enligt GDPR med avseende på, och emot, var och en av de personuppgiftsansvariga.

I händelse av konflikt mellan bestämmelser i detta arrangemang och de administrativa bestämmelserna för WIS, ska detta arrangemang äga företräde i frågor som rör personuppgiftsansvaret och behandling av personuppgifter. Arrangemanget ska tillämpas från

och med den dag då till WIS anslutande aktör bekräftar att den accepterar arrangemanget och ska gälla till dess en aktör inte längre behandlar personuppgifter i WIS.

Ändringar i arrangemanget som påkallats genomförs av MSB och gäller omgående när MSB meddelat om ändringarna på sin webbplats.

Vardera personuppgiftsansvarig ansvarar utöver att ingå detta arrangemang för att göra den dokumentation av personuppgiftsbehandling som krävs för att uppfylla principen om ansvarsskyldighet i GDPR.

2. Typ av personuppgifter som behandlas

Följande personuppgifter behandlas:

- Namn, befattning, e-post om aktörsadministratör, användare av systemet samt kontaktpersoner hos viktiga samarbetspartners,
- Användarnamn på användare som gör inloggning, samt användarnamn eller e-post för användare för att kunna få nytt tillfälligt lösenord eller efter kontakt med support.
- Namn på person som gjort notering för aktörs räkning, på den som skrivit en loggpost samt namn på alla som skrivit anteckningar som finns i loggen.
- Eventuella namn som nämns i dokument som t.ex. laddats upp i WIS av aktör eller som förekommer i kalenderposter.
- Eventuella namn i e-post hos aktör utanför WIS som får begäran om lägesrapport samt ev. namn på den som svarat på begäran/lägesrapport.

Systemet innehåller fritextfält i vilka alla sorters personuppgifter kan förekomma. De administrativa bestämmelserna för WIS poängterar dock att personuppgifter ska undvikas i så stor utsträckning som möjligt.

Inga särskilda kategorier av personuppgifter eller personuppgifter som omfattas av sekretess får förekomma i WIS.

3. Klargörande av personuppgiftsansvarigas roller

Systemet bekostas och utvecklas av MSB. WIS utvecklas i samarbete med aktörerna. MSB och aktörerna i WIS har delvis samma ändamål och medel för behandlingen av personuppgifter i WIS. Personuppgiftsansvaret är därmed huvudsakligen gemensamt. Ett gemensamt personuppgiftsansvar innebär också att de registrerades rättigheter kan tillgodoses på bästa sätt.

MSB har ensamt personuppgiftsansvaret för de personuppgiftsbehandlingar som utförs som en del i MSB:s aktörsadministration av WIS, vid anslutning av en ny aktör till systemet. Vidare har MSB ensamt personuppgiftsansvaret för driften och förvaltningen av WIS.

MSB har rätt att anlita underleverantörer samt personuppgiftsbiträden för att fullgöra driften och förvaltningen av WIS och för att kunna utföra vissa åtgärder som t.ex. att bistå vid tillägg eller borttag av användare samt vid support. MSB ansvarar för att relationen till dessa leverantörer och personuppgiftsbiträden regleras med relevanta avtal, som t.ex. personuppgiftsbiträdesavtal. Sådana leverantörer och personuppgiftsbiträden kontaktar vid behov MSB.

Aktörerna i WIS har huvudsakligen ensamt personuppgiftsansvaret för personuppgiftsbehandlingar som sker inom de ytor som skapas och används i WIS.

Hos MSB finns en centraladministration bestående av personal inom MSB samt av first line support hos MSB:s underleverantör. Syftet med centraladministrationen är att stötta aktörerna. Centraladministrationen agerar endast på begäran av en aktör.

En detaljerad uppdelning av respektive parts ansvar för varje personuppgiftsbehandling som sker vid administration och användning av WIS, finns i bilaga *SammanställIning - Personuppgiftsbehandlingar i WIS*.

Gemensam kontaktpunkt för registrerade är MSB. Om MSB blir kontaktad av en registrerad som vill utöva sina rättigheter bör MSB kontrollera med den registrerade om denne har en relation till någon aktör i WIS. Om så är fallet bör MSB meddela dels berörd aktör, dels meddela den berörda registrerade om det är bättre att den registrerade har direktkontakt med en viss aktör.

De personuppgiftsansvariga åtar sig att bistå varandra med att ge tillsynsmyndigheter eller, om det krävs enligt EU-rätten eller enligt en medlemsstats nationella rätt, annan tredje man information om en viss behandling av personuppgifter.

4. Ändamål, laglig grund och medel för personuppgiftsbehandlingen

MSB och aktörerna i WIS har delvis samma ändamål och medel för behandlingen av personuppgifter i WIS. Ändamålen med personuppgiftsbehandlingarna i WIS är att

- administrera anslutningar av aktörer till WIS,
- skapa ytor samt bedriva arbete inom dessa ytor,
- lägga till och ta bort aktörers användare av WIS,
- exportera, avsluta och arkivera ytor i WIS.

Personuppgiftsbehandling i WIS sker för att den är nödvändig för att fullgöra arbetsuppgifter av allmänt intresse (artikel 6.1 e i GDPR) eller för att fullgöra rättsliga förpliktelser som åvilar de personuppgiftsansvariga (artikel 6.1 c i GDPR).

Medel för behandlingarna är de systemkomponenter och funktionaliteter som finns i WIS. WIS är byggt av MSB som också svarar för systemets drift, förvaltning och underhåll. I WIS finns en karttjänst. Personuppgifter behandlas endast i den bakomliggande driftdatabasen samt inom ytor i WIS. I kartfunktionen behandlas inga personuppgifter.

I, samt till och från, WIS kan personuppgifter huvudsakligen komma att, inhämtas, lagras, utlämnas via överföring, arkiveras och raderas. Arkiveringsansvar för ytor som avslutats åvilar respektive aktör i WIS. För mer detaljerad redovisning i vilka sammanhang och på vilka sätt personuppgifter behandlas samt vilken part som är personuppgiftsansvarig för respektive behandling, se bilagan *SammanställIning - Personuppgiftsbehandlingar i WIS*.

5. Säkerhet i samband med behandlingen

De personuppgiftsansvariga ska säkerställa att endast personer som behöver behandla personuppgifter för att fullgöra sina arbetsuppgifter också är de som gör det, samt att all personuppgiftsbehandling som sker i WIS är förenlig med de grundläggande principerna för dataskydd. De personuppgiftsansvariga har ansvar för att WIS används endast till det som WIS är tänkt.

När en aktör planerar att hämta in information till en yta som den verkar inom, ska aktören påminna den som ska lämna informationen att minimera mängden personuppgifter. Aktören ska även se över vilka användare av WIS som är aktuella och som kan tas bort löpande.

MSB ansvarar för informationssäkerheten i WIS. MSB ska genomföra riskanalyser löpande och implementera lämpliga tekniska och organisatoriska åtgärder i syfte att säkerställa att alla åtgärder vidtagits som krävs i enlighet med artikel 32 i GDPR.

Personuppgiftsansvariga ska dokumentera de säkerhetsåtgärder som vidtagits enligt ovan. Respektive personuppgiftsansvarig ska informera den andre om förändringar, förhållanden eller andra omständigheter som kan påverka vidtagna informationssäkerhetsåtgärder eller behovet av sådana skydd.

6. Hur registrerade kan utöva sina rättigheter

För att utöva sina rättigheter kan den registrerade i första hand vända sig till den aktör i WIS som den registrerade har en relation till. Den registrerade får dock alltid utöva sina rättigheter enligt GDPR med avseende på, och emot, var och en av de personuppgiftsansvariga.

De personuppgiftsansvariga ska vid behov bistå varandra vid fullgörandet av skyldigheterna om att tillgodose den registrerades rättigheter i enlighet med kap III i GDPR. Bland annat i fråga om rätten till information, rätten till rättelse, rätten till radering eller begränsning av behandlingen, rätten till invändning och rätten till tillgång till de personuppgifter som behandlas.

Personuppgiftsansvarig åtar sig att utan dröjsmål, senast inom 30 dagar, vidta rättelse av felaktiga eller ofullständiga personuppgifter efter begäran från registrerade som inkommit till den andre personuppgiftsansvarige.

De personuppgiftsansvariga kommer inte alltid att kunna tillmötesgå begäran om radering av personuppgifter i de fall personuppgiftsbehandlingen har tillkommit för att uppfylla en rättslig förpliktelse eller för att utföra en uppgift av allmänt intresse. Förutom i fall enligt artikel 17 punkten 3 i GDPR ska respektive personuppgiftsansvariga vid beslut om radering eller förstöring av personuppgifter avlägsna dessa permanent från alla lagringsmedier som personuppgiftsansvarig förfogar över. Detta ska ske utan onödigt dröjsmål efter beslut om radering.

Respektive personuppgiftsansvariga ska skicka en skriftlig bekräftelse på att rättelse eller radering/förstöring har skett till den andre personuppgiftsansvarige inom 30 dagar efter att åtgärder vidtagits.

7. Information till registrerade

Respektive personuppgiftsansvarig ansvarar för att informera registrerade som berörs av respektive personuppgiftsansvarigs behandlingar av personuppgifter, t.ex. då inhämtande av information sker och personuppgifter då förekommer eller då en ny användare i WIS läggs till.

Detta arrangemang ska göras tillgängligt för de registrerade. Detta görs via MSB:s och respektive aktörs webbplatser.

8. Hantering och anmälan av personuppgiftsincidenter till tillsynsmyndigheten

En aktör som upptäcker en personuppgiftsincident ska utan onödigt dröjsmål meddela MSB detta. Om MSB upptäcker en personuppgiftsincident ska MSB utan onödigt dröjsmål meddela den eller de aktörer som berörs av incidenten.

De personuppgiftsansvariga ska gemensamt arbeta för att stoppa incidenten, begränsa dess verkningar, göra en eventuell anmälan till Integritetsskyddsmyndigheten (IMY) samt genomföra eventuella informationsinsatser gentemot registrerade.

Vid behov ska MSB:s och aktörens dataskyddsombud samverka för att vidta åtgärder med anledning av en inträffad incident.

9. Skyldigheter efter arrangemangets upphörande

Varje personuppgiftsansvarig som fört in och behandlat personuppgifter i en yta har inför avslut och borttag av en yta ansvar för att, beroende på vad aktören själv har för behov av personuppgifterna i fråga och beroende på hur arkivansvaret fördelats mellan aktörer i WIS, exportera personuppgifterna som behandlats om dessa behöver behandlas för andra ändamål, t.ex. arkiveringsändamål. Aktören har också ett ansvar att radera eventuella kvarvarande personuppgifter som aktören fört in och behandlat i en yta. Aktören bär personuppgiftsansvar för detta.

När MSB agerar som aktör gäller ovanstående på samma sätt för MSB.

MSB har ansvar för att vid avslut och borttag av ytor för att personuppgifterna i den bakomliggande databasen raderas. MSB bär personuppgiftsansvar för detta.

Samtliga åtgärder inför avslut och borttag av ytor ska ske i enlighet med de administrativa bestämmelserna i WIS.

MSB ska säkerställa att inga personuppgifter finns kvar hos MSB eller i tillämpliga fall MSB:s underbiträden, såvida det inte finns en skyldighet att lagra personuppgifterna enligt unionsrätten eller nationell rätt.

10. Ansvar för skada i samband med behandling

Vid fråga om ersättning för skada i samband med personuppgiftsbehandling som kan komma att utgå till en registrerad på grund av överträdelse av tillämplig bestämmelse i GDPR eller dataskyddslagen ska art. 82 i GDPR tillämpas.

Om ansvarsanspråk riktas mot någon av personuppgiftsansvariga för skada där parterna har ett solidariskt ansvar enligt vad som anges i artikel 82 p.4 och 5 i GDPR och

denna part därmed kan komma att behöva betala full ersättning till en registrerad, ska parten som hålls ansvarig omedelbart meddela motparten om det uppkomna ansvaret samt vilken behandling som orsakat skadan.

11. Giltighetstid, omförhandling och skyldighet att meddela behandling i strid med bl.a. detta arrangemang

Arrangemanget gäller från den tidpunkt som den personuppgiftsansvarige är ansluten till WIS och behandlar personuppgifter i systemet till dess den personuppgiftsansvariges personuppgiftsbehandling i WIS inte längre pågår, vid vilken tidpunkt detta arrangemang upphör att gälla utan föregående uppsägning.

Båda parter kan begära omförhandling av arrangemanget vid relevanta ändringar i dataskyddslagstiftningen. Sådan begäran om omförhandling ska göras skriftligen.

Om någon av parterna får kännedom om att motparten agerar i strid med arrangemanget, de administrativa bestämmelserna och/eller tillämplig dataskyddslagstiftning, ska den parten utan dröjsmål meddela motparten om detta. Därefter äger parten rätt att med omedelbar verkan upphöra att utföra sina förpliktelser enligt arrangemanget till den tidpunkt motparten förklarat att agerandet upphört och förklaringen accepterats av den part som påtalat agerandet.