Myndigheten
för civilt försvar

Allmänna villkor MISP-SE

Innehållsförteckning

Allmänna villkor MISP-SE **1**

Innehållsförteckning **1**

Introduktion **2**

Definitioner **2**

Syfte och målsättning med MISP-SE **2**

Medlemskap i MISP-SE **3**
Medlemsorganisationer 3

Anslutning till MISP-SE **3**

Grundläggande villkor **4**
Tillit och förtroende 4
Publicering av information 4
Användning av information 5

Uppförandekod **5**

Finansiering **5**

Myndigheten för civilt försvars rättigheter som huvudman för MISP-SE **6**

Information i MISP-SE och utlämningsärenden **6**

Ansvar för behandling av personuppgifter i MISP-SE **7**

Säkerhetsincidenter **7**

Ändring av dessa villkor **8**

Bilaga 1. Gemensamt personuppgiftsansvar i MISP-SE **8**

Versionshantering

Version	Datum	Vad	Vem
1.0	2025-03-05	Version 1.0	AB
1.1	2025-12-05	Bearbetning av dokumentet som helhet. Ny text om personuppgiftsansvar och anslutning.	HR
1.2	2026-01-26	Tillägg om Myndigheten för civilt försvars personuppgiftsbehandling samt krav på översyn av användarbehörigheter. Ändring från ”MSB” till ” Myndigheten för civilt försvar”.	HR

Introduktion

Myndigheten för civilt försvar förvaltar och utvecklar MISP-SE, en nationell nod för informationsutbyte. Den nationella noden är uppsatt genom open source plattformen Malware Information Sharing Platform (MISP) som möjliggör utbyte av teknisk information om it-säkerhetsincidenter mellan organisationer. Myndigheter, regioner, kommuner och privata aktörer som uppfyller villkoren för medlemskap får ansluta sig till MISP-SE kostnadsfritt.

Syftet med detta dokument är att tydliggöra de regler och villkor som gäller för både den organisation och dess användare som önskar ansluta till MISP-SE.

Definitioner

MISP-SE: Den MISP-instans som tillhandahålls av Myndigheten för civilt försvar och som utgör Sveriges nationella nod för informationsutbyte.

Medlemsorganisationer: Organisation som blivit godkänd som medlem i MISP-SE.

Användare: Användare är enligt dessa användarvillkor alla personer, som har tilldelats ett användarkonto. Registrerade användare kan bara vara fysiska personer med full rättskapacitet, med undantag för ett användarkonto per organisation för automatiskt datautbyte mellan organisationens MISP-instans och MISP-SE.

Syfte och målsättning med MISP-SE

Syftet med MISP-SE är att stärka Sveriges samlade motståndskraft mot cyberangrepp genom delning av hotinformation mellan verksamhetsutövare. Målsättningen är att utgöra en nationell toppnod i ett ekosystem för strukturerad

informationsdelning i realtid, som bidrar till att fler verksamhetsutövare tillgodogör sig och delar agerbar hotinformation.

Medlemskap i MISP-SE

För medlemskap krävs att organisationen godkänner villkoren i detta dokument. Om en organisation inte efterlever gällande villkor och krav riskerar organisationen att uteslutas från MISP-SE. Det är upp till Myndigheten för civilt försvar att göra den bedömningen.

Medlemsorganisationer

För att bli medlem i MISP-SE ska organisationen vara etablerad i Sverige. Medlemskap kan beviljas organisationer som:

- Bedriver skyddsvärd verksamhet enligt § 3 lag (2023:560) om granskning av utländska direktinvesteringar.
- Omfattas av 3–8 §§ i Cybersäkerhetslag (2025:1506)
- Är en statlig myndighet.
- Levererar väsentlig it-drift och/eller säkerhetslösningar till organisationer som omfattas av ovan.

Kriterierna för medlemskap kan komma att utvidgas i ett senare skede av etableringen av MISP-SE.

Anslutning till MISP-SE

Medlemsorganisationer kan välja att få tillgång till MISP-SE antingen genom att logga in i webbgränssnittet för att hantera data direkt i webbläsaren, eller genom synk mellan en egen MISP och MISP-SE.

För att ansluta till MISP-SE krävs att organisationen använder en statisk IP-adress som är registrerad i Sverige enligt RIPE:s register. Detta gäller för båda anslutningsalternativ som beskrivs ovan.

Det uppmuntras att andra MISP-sammanslutningar, såsom sektorsMISP eller motsvarande, ansluter sig till MISP-SE. Samtliga organisationer i den anslutande MISP-sammanslutningen, såväl befintliga som tillkommande, måste godkännas som medlemmar i MISP-SE.

Grundläggande villkor

För att uppnå syftet med MISP-SE krävs ett klimat som kännetecknas av en kombination av balans mellan öppenhet, enkelhet och förtroende. För att skapa förutsättningar för detta **ska** medlemsorganisationer efterleva nedanstående villkor.

Tillit och förtroende

- Medlemsorganisationers säkerhetsarbete ska i allt väsentligt motsvara den nivå som följer av Cybersäkerhetslagen och/eller ISO 27001/2 i syfte att obehöriga inte får tillgång till information i MISP-SE.
- Medlemsorganisationer som ansluter sig via API ska säkerställa ett ändamålsenligt skydd av sin egen MISP-instans utifrån en dokumenterad riskanalys.
- Medlemsorganisationer som ansluter sig via API ska säkerställa att den egna organisationens MISP hålls uppdaterad.
- Medlemsorganisationerna ansvarar för att deras användare har kännedom om och följer gällande villkor.
- Den anslutna organisationen ansvarar för att regelbundet se över och uppdatera sina användarbehörigheter.
- Användare som ansluter gör det endast i sin roll inom den anslutna organisationen samt från organisationens utrustning.
- Alla aktiviteter i MISP-SE är förbjudna som skadar tredje parters rättigheter.

Publicering av information

- Den som delar information i MISP-SE gör det med goda avsikter. Detta innebär att information som delas genom MISP-SE görs i syfte att skydda och dela information relaterat till cybersäkerhet.
- Den information som delas är inte behäftad med immateriella rättigheter som tillkommer någon annan.
- Information som delas i MISP-SE är kvalitetskontrollerad och följer reglerna för informationsdelning i *Arbetssätt och Rutiner MISP-SE*.
- I MISP-SE delas inte information som är säkerhetsskyddsklassad och som omfattas av bestämmelser i säkerhetsskyddslag (2018:585).
- I MISP-SE återpubliceras inte OSINT[1] utan adderad bearbetning/analys av användaren. I undantagsfall kan detta göras, om informationen bedöms som relevant för andra medlemmar.
- Genom att publicera information i MISP-SE ges andra medlemmar rätt att använda informationen i säkerhetssyften, eventuellt utifrån definierade begränsningar, vilka ska framgå av eventet.

[1] Open source intelligence.

- Det är förbjudet att dela känsliga personuppgifter. Andra personuppgifter får delas om det är förenligt med gällande dataskyddslagstiftning och är nödvändigt för MISP-SE:s syfte.

Användning av information

- Varje organisation vidtar åtgärder utifrån informationen i MISP-SE på eget ansvar. Detta innebär att Myndigheten för civilt försvar inte tar något ansvar för negativa effekter av något slag som härrör från åtgärder som vidtagits utifrån information som distribuerats genom MISP-SE.
- Informationen i MISP-SE får inte delas utanför EU/EES.

Uppförandekod

Det är avgörande att MISP-SE blir värdefull för alla parter, vilket kräver att uppförandekoden efterlevs. MISP-SE ska kännetecknas av ett professionellt och respektfullt klimat, som främjar samarbete och nytta. Därför är det viktigt att upprätthålla principer som kännetecknas av:

- Att använda ett välkomnande och inkluderande språk.
- Att visa respekt för olika synpunkter och erfarenheter.
- Att fokusera på vad som är bäst för samhället.
- Att samarbeta med, och förhålla sig till, andra organisationer i MISP-gemenskapen.

Myndigheten för civilt försvar, i egenskap av organisation som tillhandahåller MISP-SE, förväntas vidta korrigerande åtgärder som svar på alla fall av ovälkommet beteende.

Finansiering

Myndigheten för civilt försvar finansierar drift, förvaltning, support och utveckling kopplat till MISP-SE.

Deltagande i MISP-SE och eventuella samarbetsforum kring MISP-SE sker på frivillig basis. Medlemsorganisationer står för sina egna kostnader kopplat till användningen av MISP-SE.

Myndigheten för civilt försvars rättigheter som huvudman för MISP-SE

Myndigheten för civilt försvar har rätten att godkänna nya medlemmar i MISP-SE. Vidare kan Myndigheten för civilt försvar ta bort, redigera eller avvisa kommentarer, åtaganden, kod, problem och annat tillgängligt innehåll i MISP-SE som inte är i linje med villkoren eller uppförandekoden. Genom medlemsorganisationens anslutning till MISP-SE ges Myndigheten för civilt försvar en avgiftsfri, icke-exklusiv, i tiden obegränsad nyttjanderätt till den information som delas. Informationen ska också kunna delas vidare till andra medlemmar och organisationer, såväl inom som utanför MISP-SE, under förutsättning att detta sker i enlighet med av syftet med MISP-SE.

Det är av högsta vikt att reglerna för klassificering och informationsdelning följs för att MISP-gemenskapen ska fungera. Om en organisation inte följer dessa regler, förbehåller Myndigheten för civilt försvar sig rätten att genast utesluta respektive användare, eventuellt ansvarig Org-Admin eller hela organisationen från MISP-plattformen. Även andra avvikelser gentemot *Allmänna villkor MISP-SE* kan resultera i uteslutning. Uteslutning kan ske tillfälligt eller permanent. Beroende på karaktären av regelbrottet kan uteslutning ske utan föregående meddelande.

Information i MISP-SE och utlämningsärenden

Information som publiceras i MISP-SE kommer att betraktas som inkommen handling till de myndigheter, inklusive Myndigheten för civilt försvar, som är anslutna till MISP-SE. Vid ett eventuellt utlämningsärende gör den berörda myndigheten en bedömning om informationen kan lämnas ut. I samband med denna bedömning bör berörd myndighet samråda med den medlemsorganisation som publicerat informationen.

Ansvar för behandling av personuppgifter i MISP-SE

Medlemsorganisationerna och Myndigheten för civilt försvar är var för sig ensamt personuppgiftsansvariga för de behandlingar av personuppgifter som sker inom MISP-SE för den egna verksamheten och för egna ändamål.

Myndigheten för civilt försvar är ensamt personuppgiftsansvarig för behandlingar av personuppgifter som utförs som en del i Myndigheten för civilt försvars aktörsadministration av MISP-SE samt för driften och förvaltningen av MISP-SE.

I det fall en medlemsorganisation säger upp sitt medlemskap i MISP-SE kommer behandlingen av organisationens personuppgifter för medlemskap att avslutas så snart som möjligt. Personuppgifterna kommer att gallras, såvida detta inte strider mot gällande arkivlagstiftning. Om uppgifterna behöver bevaras kommer de att avskiljas för arkivering.

Viss personuppgiftsbehandling inom MISP-SE kan komma att ske med helt eller delvis samma ändamål och medel för behandlingen av personuppgifter. Myndigheten för civilt försvar och den medlemsorganisation behandlingen rör har i dessa fall ett gemensamt personuppgiftsansvar för den aktuella behandlingen. Uppdelningen av ansvaret för personuppgifter finns dokumenterat i bilaga 1 ”Gemensamt personuppgiftsansvar MISP-SE”. Dokumenten finns på Myndigheten för civilt försvars webbplats. Tillsammans utgör dessa handlingar ett sådant arrangemang om gemensamt personuppgiftsansvar som följer av dataskyddsförordningen, artikel 26.

Genom att ansluta sig som medlem i MISP-SE åtar sig medlemsorganisationen att följa arrangemanget om gemensamt personuppgiftsansvar.

Säkerhetsincidenter

Om användaren skulle få kännedom om en säkerhetsincident avseende MISP-SE, ska denna omgående anmälas till Myndigheten för civilt försvar.

Exempel på säkerhetsincidenter som ska anmälas till Myndigheten för civilt försvar är när:

- De direkt berör MISP-SE (såsom kompromettterade användarkonton).
- De berör andra system, om innehåll behandlas på dessa, som mottagits av MISP-SE (såsom dataläckage på en anknuten MISP-server).

Observera att förteckningen inte är uttömmande och att andra, särskilt lagenliga anmälningsplikter, inte berörs.

Ändring av dessa villkor

Myndigheten för civilt försvar har rätten att ändra dessa villkor. Vid ändring ska anslutna organisationer meddelas om ändringen.

Ändringar i *Allmänna villkor MISP-SE* kan också initieras av en ansluten organisation. Förslag skickas då till Myndigheten för civilt försvar som behandlar förslaget och återkopplar till initierande organisation.

Bilaga 1. Gemensamt personuppgiftsansvar i MISP-SE

Bakgrund och syfte

Myndigheten för civilt försvar förvaltar och utvecklar MISP-SE, en nationell nod för informationsutbyte. Syftet med MISP-SE är att stärka Sveriges samlade motståndskraft mot cyberangrepp genom delning av hotinformation mellan verksamhetsutövare.

Den nationella noden är uppsatt genom open source plattformen Malware Information Sharing Platform (MISP) som möjliggör utbyte av teknisk information om cyberhot mellan organisationer. Myndigheter, regioner, kommuner och privata medlemsorganisationer som uppfyller villkoren för medlemskap får ansluta sig till MISP-SE.

Viss personuppgiftsbehandling inom MISP-SE kan komma att ske med helt eller delvis samma ändamål och medel för behandlingen av personuppgifter. Myndigheten för civilt försvar och den medlemsorganisation behandlingen rör har i dessa fall ett gemensamt personuppgiftsansvar för den aktuella behandlingen. Denna handling utgör ett sådant arrangemang om gemensamt personuppgiftsansvar som följer av artikel 26 GDPR.

Grundläggande bestämmelser

Genom att ansluta sig som medlem i MISP-SE åtar sig medlemsorganisationen att följa *Allmänna villkor MISP-SE*, gällande dataskyddslagstiftning samt detta arrangemang om gemensamt personuppgiftsansvar.

I händelse av konflikt mellan bestämmelser i detta arrangemang och de allmänna villkoren för MISP-SE ska detta arrangemang äga företräde i frågor som rör personuppgiftsansvaret och behandling av personuppgifter.

Arrangemanget ska tillämpas från och med den dag då medlemsorganisationen ansluts till MISP-SE och gäller till dess medlemsorganisationen inte längre behandlar personuppgifter vilka erhållits genom MISP-SE eller delats genom MISP-SE.

Ändringar i arrangemanget som påkallats genomförs av Myndigheten för civilt försvar och gäller omgående när Myndigheten för civilt försvar meddelat om ändringarna på sin webbplats.

Vardera personuppgiftsansvarig ansvarar utöver att ingå detta arrangemang för att göra de åtgärder som krävs vid personuppgiftsbehandling enligt gällande dataskyddslagstiftning, inklusive men inte begränsat till skyldigheter rörande dokumentation, register och information till registrerade.

Typ av personuppgifter som behandlas

- Namn, e-post, telefonnummer, användarnamn för medlemsorganisationsadministratör och användare av MISP-SE.
- *Användarnamn på användare som gör inloggning, samt användarnamn eller epost för användare för att kunna få nytt tillfälligt lösenord eller efter kontakt med kundtjänst.*
- Beroende på autentiseringsmetod kan även Unikt ID för mobila autentiserings-applikationer behandlas.
- IP-adresser, e-postadresser, domännamn och andra möjliga personuppgifter som används som IOC:er[2].
- Eventuella namn som nämns i dokument som t.ex. laddats upp i MISP-SE av medlemsorganisation.

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

Klargörande av personuppgiftsansvarigas roller

Detta arrangemang återspeglar de gemensamt personuppgiftsansvarigas respektive roller och förhållanden gentemot varandra och de registrerade.

Ensamt personuppgiftsansvar

Medlemsorganisationerna och Myndigheten för civilt försvar är var för sig ensamt personuppgiftsansvariga för de behandlingar av personuppgifter som sker inom MISP-SE för den egna verksamheten och för egna ändamål.

Myndigheten för civilt försvar är därtill ensamt personuppgiftsansvarig för behandlingar av personuppgifter som utförs som en del i Myndigheten för civilt försvars medlemsadministration av MISP-SE samt för driften och förvaltningen av MISP-SE. Myndigheten för civilt försvar har rätt att anlita leverantörer/personuppgiftsbiträden för att fullgöra driften och förvaltningen av MISP-SE samt för att kunna utföra nödvändiga åtgärder i systemet. Myndigheten för civilt försvar ansvarar för att relationen till dessa leverantörer/ personuppgiftsbiträden regleras med relevanta avtal, inklusive tillräckligt

[2] Indicator of compromise.

personuppgiftsbiträdesavtal. Leverantörer/ personuppgiftsbiträden ska vid behov kontakta Myndigheten för civilt försvar direkt, även i de fall behovet uppstått i samband med en medlems nyttjande av MISP-SE.

Gemensamt personuppgiftsansvar

Myndigheten för civilt försvar och respektive medlemsorganisation har gemensamt personuppgiftsansvar till den del de har samma ändamål och medel för en viss behandlingen av personuppgifter i MISP-SE. Om Myndigheten för civilt försvar eller någon av medlemsorganisationerna finner att så är fallet ska en särskild Specifikation upprättas mellan parterna.

Gemensam kontaktpunkt för de registrerade i dessa fall är Myndigheten för civilt försvar. Om Myndigheten för civilt försvar blir kontaktad av en registrerad som vill utöva sina rättigheter bör Myndigheten för civilt försvar kontrollera med den registrerade om denne har en relation till någon medlemsorganisation i MISP-SE. Om så är fallet bör Myndigheten för civilt försvar meddela dels berörd medlemsorganisation, dels meddela den berörda registrerade om det är bättre att den registrerade har direktkontakt med medlemsorganisationen.

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.

Ändamål, laglig grund och medel för den gemensamma personuppgiftsbehandlingen

Personuppgiftsbehandling för Myndigheten för civilt försvar i MISP-SE 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).

Personuppgiftsbehandling för enskilda medlemsorganisationer i MISP-SE kommer att anges i den Specifikation som ska tas fram mellan parterna i det fall ett gemensamt personuppgiftsansvar anses föreligga.

Medel för behandlingarna är de systemkomponenter och funktionaliteter som finns i MISP-SE.

I, samt till och från, MISP-SE kan personuppgifter huvudsakligen komma att samlas in, lagras, analyseras, delas via överföring och raderas.

Säkerhet i samband med behandlingen

Den 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 MISP-SE är förenlig med gällande dataskyddsslagstiftning.

Den personuppgiftsansvariga har ansvar för att MISP-SE används endast till det som MISP-SE är tänkt.

När en medlemsorganisation planerar att hämta in information till en yta som den verkar inom, ska medlemsorganisationen påminna den som ska lämna informationen att minimera mängden personuppgifter.

Myndigheten för civilt försvar ansvarar för informationssäkerheten i MISP-SE. Myndigheten för civilt försvar 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 vid gemensamt personuppgiftsansvar informera den andre om förändringar, förhållanden eller andra omständigheter som kan påverka vidtagna informationssäkerhetsåtgärder eller behovet av sådana skydd.

Hur registrerade kan utöva sina rättigheter

För att utöva sina rättigheter kan den registrerade i första hand vända sig till den medlemsorganisation 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.

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

Vid gemensamt personuppgiftsansvar ska mottagaren av begäran om rättelse eller radering skicka en skriftlig bekräftelse på att rättelse eller radering/förstöring har skett till den andre personuppgifts-ansvarige inom 30 dagar efter att åtgärder vidtagits.

Hantering och anmälan av personuppgiftsincidenter till tillsynsmyndigheten

Den som upptäcker en personuppgiftsincident ska utan onödigt dröjsmål meddela Myndigheten för civilt försvar detta. Om Myndigheten för civilt försvar upptäcker en personuppgiftsincident ska Myndigheten för civilt försvar utan onödigt dröjsmål meddela den eller de medlemsorganisationer 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 Myndigheten för civilt försvars och medlemsorganisationens dataskyddsombud samverka för att vidta åtgärder med anledning av en inträffad incident.

Skyldigheter efter arrangemangets upphörande

Varje personuppgiftsansvarig som behandlat personuppgifter i MISP-SE har inför avslut skyldighet att exportera personuppgifterna som behandlats om dessa behöver behandlas för andra ändamål, t.ex. arkiveringsändamål. Den personuppgiftsansvarige har också ett ansvar att radera eventuella kvarvarande personuppgifter.

Samtliga åtgärder inför avslut och borttag av ytor ska ske i enlighet med Allmänna villkor.

Myndigheten för civilt försvar ska säkerställa att inga personuppgifter finns kvar hos Myndigheten för civilt försvar eller i tillämpliga fall Myndigheten för civilt försvars biträden, såvida det inte finns en skyldighet att lagra personuppgifterna enligt unionsrätten eller nationell rätt.

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 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.

Den part som orsakat en skada med anledning av en överträdelse av tillämplig bestämmelse i GDPR ska dock hålla motparten skadeslös. Begäran om ersättning

för uppkommen skada ska sändas inom 30 dagar från det att parten meddelas skadans omfattning.

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 MISP-SE och behandlar personuppgifter i systemet till dess den personuppgiftsansvariges personuppgifts-behandling i MISP-SE 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, Allmänna villkor 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.