

Svar från Bakgrundskontrollföretagen på enkät om behovet av bakgrundskontroller

Avseende utredningen om bakgrundskontroller, Ju 2025:19

1. Närmare om respondenten

1.1 Är ni verksamma inom offentlig eller privat sektor?

Privat sektor.

Bakgrundskontrollföretagen (BKF) är en branschorganisation för professionella leverantörer av bakgrundskontroller och relaterade riskbedömningar till både offentlig och privat sektor. Medlemsföretagen verkar inom samtliga branscher och bistår arbetsgivare och uppdragsgivare i riskexponerade beslutssituationer.

BKF fungerar som en samlade, normbildande och kvalitetssäkrande instans för seriösa aktörer på marknaden. Den samlade erfarenheten från medlemsföretag och deras kunder är att hotbilden mot arbetsgivare, samhällsviktiga verksamheter och affärsrelationer har ökat, samtidigt som regelverk och tillgång till relevanta uppgifter är fragmenterade, svårtolkade och i vissa delar otidsenliga.

Branschen utgår från en risk- och befattningsbaserad proportionalitetsprincip, där mer skyddsvärda roller och relationer motiverar mer fördjupade kontroller. Integritetsskyddet stärks i praktiken när bakgrundskontroller genomförs av professionella aktörer med etablerad metodik, dataminimering, spårbarhet och strukturerad relevansbedömning, jämfört med informella eller ad hoc-kontroller hos enskilda uppdragsgivare.

1.2 Vilken typ verksamhet bedrivs?

BKF:s medlemsföretag bedriver verksamhet inom personalsäkerhet och affärsrisk. Detta omfattar bakgrundskontroller inför och under anställning samt granskningar kopplade till affärs- och avtalsrelationer, såsom leverantörer, samarbetspartners, konsulter och andra kritiska relationer.

Verksamheten är inriktad på att stödja legitima arbetsgivare och uppdragsgivare i strukturerad riskhantering. BKF:s medlemsföretag utför inte kontroller för privatpersoner eller i situationer där det saknas berättigat och dokumenterat ändamål. Uppdragen förutsätter alltid ett tydligt syfte kopplat till verksamhetsrisk, ansvar och skyddsvärde.

Utöver beslutsstöd inför ingående av relationer omfattar verksamheten även löpande riskstyrning, exempelvis vid förändrade roller, befordran, utökad åtkomst, organisationsförändringar eller inträffade incidenter.

1.3 Hur stor är organisationen, ungefär hur många personer är anställda eller deltar i verksamheten på motsvarande sätt som anställda?

BKF är en branschorganisation vars medlemsföretag varierar i storlek. Sammantaget omfattar medlemsföretagen ett betydande antal specialister såsom analytiker, researchers, och ledning.

Gemensamt är att verksamheten bedrivs genom standardiserade och kvalitetssäkrade processer med tydlig spårbarhet, vilket är avgörande vid hantering av integritetskänsliga uppgifter och vid rättssäkra riskbedömningar.

1.4 Hur många rekryteringar sker per år? Vid hur stor andel av rekryteringarna görs någon form av bakgrundskontroll?

BKF:s medlemsföretag genomför tillsammans mycket stora volymer bakgrundskontroller årligen, motsvarande flera tiotusentals kontroller. För uppdragsgivarna görs mer omfattande bakgrundskontroller i en hög andel av rekryteringar där roller bedöms vara i högre grad riskexponerade, medan lågriskroller normalt hanteras genom mindre omfattande bakgrundskontroller.

Medlemsföretagens kunder beskriver ett tydligt glapp mellan upplevt behov och faktisk tillämpning. Efterfrågan på bakgrundskontroller ökar, men rättslig osäkerhet och otydliga ramar gör att kontroller ibland inte genomförs trots reella risker.

1.5 Finns det beträffande verksamheten en rätt enligt befintliga författningar att få del av uppgifter ur belastningsregistret och/eller misstankeregistret inför anställning av viss personal?

BKF:s medlemsföretag har i sig ingen generell rätt att få del av belastnings- eller misstankeregister. Arbetsgivare och uppdragsgivare saknar i många fall författningsstöd för registerutdrag utanför särskilt reglerade sektorer.

Information om lagöverträdelser inhämtas därför i stället genom exempelvis domstolshandlingar. Medlemsföretag och kunder beskriver att nuvarande ordning i praktiken leder till osäkerhet, muntlig hantering och svårigheter att dokumentera riskbedömningar, vilket kan försvaga både rättssäkerhet och integritetsskydd.

1.5.1 Om ja, med stöd av vilken författning och i vilka situationer finns en sådan rätt till registerutdrag?

Exempel på särskilda regelverk där uppdragsgivare kan omfattas av rätt till registerutdrag är bland annat:

- Lag (2013:852) om registerkontroll av personer som ska arbeta med barn
- Lag (2018:1219) om försäkringsdistribution

Utanför sådana särskilt reglerade situationer saknas i regel generell rätt till registerutdrag.

2. Kartläggning av behovet av bakgrundskontroller inför och under anställning

2.1 Vilka behov ser ni att det finns av att kunna göra bakgrundskontroller inför och under anställning? I vilka situationer finns ett sådant behov? Vilka potentiella risker bedöms bakgrundskontroller kunna förhindra?

Behovet av bakgrundskontroller inför och under anställning är stort och ökande i hela samhället, både inom offentlig och privat sektor. Bakgrundskontrollföretagens medlemsföretag och deras kunder är verksamma inom samtliga branscher, däribland vård, offentlig förvaltning, fastighet, industri, it- och, finansiella funktioner samt andra samhällsviktiga och kommersiella verksamheter.

Behovet uppstår i situationer där en anställning eller ett uppdrag innebär faktisk åtkomst, inflytande eller förtroende, snarare än enbart utifrån titel eller formell roll. Särskilt tydligt är behovet i befattningar som innebär åtkomst till skyddsvärda personuppgifter, affärshemligheter eller säkerhetskänslig information, hantering av ekonomiska flöden såsom betalningar, upphandling eller firmateckning, arbete med barn, äldre eller andra skyddsvärda grupper, samt förtroendeställning eller möjlighet att påverka beslut, processer eller andra individer.

Behovet av bakgrundskontroller är branschöverskridande men tar sig olika uttryck beroende på verksamhetens art och riskprofil. Inom vård och omsorg är behovet ofta kopplat till skydd av patienter, legitimationer och tillgång till känsliga uppgifter. Inom offentlig förvaltning och annan samhällsviktig verksamhet är riskerna ofta kopplade till förtroendeställning, beslutsmandat och åtkomst till skyddsvärd information. Inom industri, fastighet och teknikverksamhet kan riskerna i högre grad vara kopplade till fysisk åtkomst, sabotage, insiderproblematik eller otillbörlig påverkan. Inom finansiella funktioner och ekonomiadministration är fokus ofta på ekonomisk brottslighet, bedrägerier och intressekonflikter. Oavsett bransch är den avgörande faktorn dock inte sektorstillhörighet i sig, utan vilken faktisk åtkomst, påverkan och vilket förtroende som följer med rollen.

Bakgrundskontroller är ett centralt förebyggande verktyg för att minska risken för infiltration, insiderproblematik, bedrägerier, välfärdsbrott, ekonomisk brottslighet, kopplingar till organiserad brottslighet samt annan otillbörlig påverkan. Medlemsföretagens kunder beskriver ett säkerhetsläge där hotaktörer i ökande grad söker utnyttja legitima organisationer genom individer i förtroende- eller åtkomstpositioner, snarare än genom direkta angrepp mot organisationen som sådan.

Risk är inte statisk. Behovet av bakgrundskontroller begränsas därför inte till rekryteringstillfället, utan uppstår även under pågående anställning. Exempel på sådana situationer är rollförändringar, befordran, utökad system- eller informationsåtkomst, förändrade ekonomiska befogenheter, organisationsförändringar eller inträffade incidenter. I dessa lägen kan förändrade förutsättningar hos individen, såsom ekonomi, bolagsengagemang eller nytillkomna lagöverträdelser, påverka riskbilden på ett sätt som inte varit känt vid anställningstillfället.

Ett återkommande budskap från medlemsföretagens kunder är att bakgrundskontroller inte primärt syftar till att identifiera enskilda ”träffar”, utan till att möjliggöra en samlad, framåtblickande och proportionerlig riskbedömning. I detta ingår att identifiera mönster, avvikelser och sårbarheter som kan vara relevanta för tillförlitlighet och förtroende, särskilt i befattningar med högt skyddsvärde. Utan möjlighet att genomföra ändamålsenliga bakgrundskontroller riskerar arbetsgivare och uppdragsgivare att antingen avstå från kontroller trots tydliga risker, eller att genomföra informella

och mindre rättssäkra kontroller. Båda dessa utfall innebär i praktiken ökade risker, både för verksamheten och för den enskildes integritet.

2.2 Vilka typer av bakgrundskontroller finns det behov av (till exempel kontroll av vissa register eller andra åtgärder)?

Det finns behov av bakgrundskontroller som möjliggör en samlad, strukturerad och riskbaserad bedömning, snarare än förenklade eller isolerade kontroller. Vilka kontroller som är motiverade ska avgöras utifrån befattningens ansvar, mandat och faktiska åtkomst till exempelvis system, information, ekonomiska flöden, fysiska miljöer eller beslutsprocesser. Utgångspunkten bör vara proportionalitet: ju större faktisk påverkan och skyddsvärde, desto större legitimt behov av fördjupade kontroller.

Vid professionella bakgrundskontroller är det inte enskilda informationspunkter som ensamma ligger till grund för bedömningen, utan den sammanvägda bilden. Avvikelse, inkonsekvenser eller bristande överensstämmelse mellan uppgifter som individen själv lämnar – exempelvis i CV eller personligt brev – och verifierbar information kan i sig utgöra relevanta riskindikatorer för tillförlitlighet och förtroende, särskilt i befattningar med högt skyddsvärde. Det är ofta mönster, kombinationer och förändringar över tid som är riskrelevanta, snarare än enskilda uppgifter.

Mot denna bakgrund finns behov av att, beroende på roll och riskprofil, kunna beakta exempelvis följande informationsområden inom ramen för en strukturerad analys:

- **Identitet** är relevant i samtliga befattningar för att säkerställa att individen är den person den utger sig för att vara och för att motverka identitetsrelaterat missbruk.
- **Ekonomiska förhållanden och betalningsförseelser** är relevanta som sårbarhetsindikatorer, särskilt i roller med ekonomiskt ansvar, upphandlingspåverkan eller möjlighet till otillbörlig påverkan.
- **Bolagsengagemang och ägarförhållanden** är relevanta i befattningar med beslutsmandat, affärsrelationer eller möjlighet att agera genom externa bolag, för att identifiera intressekonflikter, bulvanupplägg eller beroendeförhållanden.
- **Tidigare anställningar och uppdrag** är relevanta för att bedöma ansvarsnivå, rollhistorik och eventuella mönster som kan påverka lämplighet och förtroende.
- **Utbildningsmeriter**, yrkeslegitimationer och behörigheter är relevanta där formell kompetens, legitimation eller rätt att utöva yrket är en förutsättning för rollen.
- **Mediaexponering** kan i vissa fall vara relevant för att identifiera allvarliga förtroenderisker kopplade till yrkesutövning eller affärsrelationer.
- **Tidigare lagöverträdelser** är relevanta i den mån de har tydlig koppling till befattningens riskprofil, exempelvis för att identifiera bedrägeririsk, kopplingar till organiserad brottslighet eller annan påverkan på tillförlitlighet.
- **Internationella sanktionslistor** är relevanta i alla befattningar och relationer där internationella kopplingar kan förekomma, eftersom svenska verksamheter i praktiken saknar full insyn i indirekta ägar- och affärsled.

De informationskategorier som kan vara relevanta vid bakgrundskontroller utgör i sig inte något nytt fenomen. Motsvarande uppgifter används redan i andra reglerade sammanhang, exempelvis

inom finanssektorn, försäkring, upphandling och penningtvättsarbete. Utmaningen ligger inte i att uppgifterna är olämpliga, utan i att det i dag saknas en sammanhållen, rättssäker och proportionerlig modell för hur de får användas inom personalsäkerhet och närliggande riskbedömningar.

BKF upplever att den offentliga och rättsliga diskussionen om bakgrundskontroller i stor utsträckning har kommit att begränsas till frågor om lagöverträdelse och brottsuppgifter. Detta riskerar att ge en förenklad bild av vilka informationsbehov som i praktiken föreligger vid riskbaserade och proportionerliga bakgrundskontroller.

I realiteten finns ett tydligt och legitimt behov av att även kunna beakta andra typer av information som redan i dag är föremål för detaljerad reglering i lag eller förordning. Detta gäller exempelvis uppgifter från folkbokföringen, Skatteverkets skatteregister, Kronofogdemyndighetens register samt utbildnings- och examensuppgifter från Ladok. Sådan information kan vara avgörande för att bedöma identitet, behörighet, ekonomisk sårbarhet och tillförlitlighet i befattningar med högt skyddsvärde.

En framtida reglering av bakgrundskontroller bör därför inte ensidigt fokusera på lagöverträdelse, utan ta ett bredare grepp om vilka lagreglerade informationskällor som i praktiken är nödvändiga för att möjliggöra rättssäkra, träffsäkra och proportionerliga riskbedömningar.

För att säkerställa kvalitet, aktualitet och integritet är det av central betydelse att riskrelevant information, när sådan används, hämtas från tillförlitliga primärkällor. Medlemsföretagens kunder, särskilt inom offentlig sektor, efterfrågar i ökande grad att uppgifter är verifierbara, aktuella och spårbara till ansvarig myndighet. Användning av sekundära eller oreglerade databaser utan tydlig tillsyn, gallring och ansvar kan i detta avseende innebära både kvalitets- och integritetsrisker.

Samtidigt ska bakgrundskontroller inte utformas som generella masskontroller. Förteckningen över informationsområden är inte statisk utan behöver kunna anpassas över tid utifrån förändrade hot, modus och verksamhetsrisker. Endast under särskilda omständigheter är det motiverat att kontrollera många områden samtidigt; i normalfallet ska ett begränsat urval användas, styrt av riskprofil och alternativa skyddsåtgärder. Professionella bakgrundskontrollföretag har här en central roll i att analysera, filtrera och endast rapportera vidare sådant som har faktisk betydelse för riskbedömningen.

2.3 Vilka uppgifter är relevanta att undersöka i en bakgrundskontroll inför respektive under anställning? Ge gärna exempel på olika typer av problematiska omständigheter som skulle kunna komma fram.

Vilka uppgifter som är relevanta att undersöka ska avgöras genom en risk- och befattningsbaserad proportionalitetsbedömning, där hänsyn tas till rollens ansvar, mandat, faktiska åtkomst och skyddsvärde. Utgångspunkten bör vara att endast uppgifter med tydlig koppling till risk och arbetsuppgifter beaktas.

Inför anställning kan relevanta uppgifter exempelvis omfatta identitet, tidigare anställningar och uppdrag, utbildnings- och yrkesmeriter, samt behörigheter eller legitimationer där detta är en förutsättning för rollen. Ekonomiska förhållanden och betalningsförseelser kan vara relevanta som sårbarhetsindikatorer, särskilt i roller med ekonomiskt ansvar eller möjlighet till påverkan. Bolagsengagemang och ägarförhållanden kan vara relevanta för att identifiera intressekonflikter eller beroendeförhållanden. Uppgifter om tidigare lagöverträdelse kan vara relevanta i den mån de har tydlig koppling till befattningens riskprofil, exempelvis avseende bedrägeri, förtroendebrott eller kopplingar till organiserad brottslighet. Mediaexponering kan i vissa fall bidra till att identifiera allvarliga förtroenderisker.

Under pågående anställning kan det fortsatt vara relevant att beakta uppgifter som kan ha förändrats över tid och som påverkar riskbilden. Detta kan exempelvis avse förändringar i ekonomisk situation, nytillkomna lagöverträdelse, nya eller förändrade bolagsengagemang, förlorade eller ändrade legitimationer och behörigheter, eller förändrad faktisk åtkomst till system och information. Problematiska omständigheter utgörs ofta av mönster, upprepade avvikelser eller kombinationer av faktorer snarare än enstaka händelser.

I båda fallen bör professionella bakgrundskontrollföretag analysera och filtrera information så att endast uppgifter med faktisk relevans för riskbedömningen rapporteras vidare. Uppgifter som saknar tydlig koppling till risk eller arbetsuppgifter, såsom enstaka mindre förseelser, bör i normalfallet inte ligga till grund för bedömning eller åtgärd.

2.4 Använder ni er av bakgrundskontroller inför respektive under anställning i dag? Utför ni i så fall bakgrundskontroller själva eller anlitas en extern aktör?

Bakgrundskontroller används i dag i betydande omfattning inför anställning, framför allt i roller som bedöms vara riskexponerade. Detta gäller såväl privat som offentlig sektor och inom ett brett spektrum av branscher. Medlemsföretagens kunder beskriver att bakgrundskontroller inför rekrytering i dag ofta uppfattas som en etablerad del av riskhanteringen när det finns tydlig koppling till ansvar, åtkomst eller förtroende.

Under pågående anställning genomförs bakgrundskontroller i betydligt mer begränsad omfattning. Samtidigt upplever många arbetsgivare att behovet av uppföljande kontroller i praktiken är större än vad som faktiskt genomförs. Detta gäller särskilt vid förändrade roller, befordran, utökad systemåtkomst eller efter inträffade incidenter. Skillnaden mellan identifierat behov och faktisk tillämpning beskrivs återkommande av medlemsföretagens kunder.

Bakgrundskontroller utförs i huvudsak genom externa, specialiserade bakgrundskontrollföretag. Skälen till detta är flera. Många arbetsgivare saknar egen kompetens att genomföra strukturerade risk- och proportionalitetsbedömningar samt att analysera information på ett rättssäkert sätt. Externa aktörer kan tillföra metodik, kvalitetssäkring och spårbarhet, samt bidra till att filtrera bort information som saknar relevans för riskbedömningen.

Ur ett integritetsperspektiv upplever många kunder att användning av professionella bakgrundskontrollföretag innebär ett stärkt skydd för den enskilde, jämfört med att arbetsgivare själva genomför informella kontroller eller inhämtar uppgifter utan tydliga ramar. Samtidigt anges rättslig osäkerhet och brist på tydlig vägledning som de främsta orsakerna till att uppföljande kontroller under anställning i dag används i begränsad omfattning.

2.5 Om uppgifter av relevans skulle komma fram vid en bakgrunds kontroll i en rekryteringsprocess, hur anser ni att uppgifterna bör hanteras?

Om uppgifter av relevans framkommer vid en bakgrunds kontroll i en rekryteringsprocess bör arbetsgivarens hantering utgå från en saklig, riskbaserad och proportionerlig bedömning. Uppgifterna ska inte leda till automatiska eller schablonmässiga beslut, utan utgöra ett beslutsunderlag som vägs samman med övrig information i rekryteringsprocessen, i linje med grundläggande arbetsrättsliga principer om saklighet och proportionalitet.

Hanteringen bör vara framåtblickande och ta hänsyn till uppgifternas art, aktualitet och koppling till befattningens ansvar, mandat och skyddsvärde. Det är särskilt viktigt att bedöma om uppgifterna indikerar ett mönster eller en samlad riskbild, snarare än att fästa avgörande vikt vid enskilda isolerade omständigheter.

Om arbetsgivaren överväger att vidta en negativ åtgärd till följd av uppgifter som framkommit i bakgrundskontrollen bör detta ske inom ramen för en tydlig och rättssäker beslutsprocess. Det bör övervägas att ställa krav på att den kontrollerade, innan ett slutligt beslut fattas, informeras om att vissa uppgifter kan påverka beslutet och ges reell möjlighet att bemöta, förklara eller korrigera uppgifterna. En sådan ordning stärker både rättssäkerheten och kvaliteten i beslutsunderlaget.

Internationella regelverk illustrerar värdet av denna typ av processuella skydd. Ett exempel är den amerikanska Fair Credit Reporting Act (FCRA), som ställer krav på att individer ges möjlighet att ta del av och bemöta uppgifter innan ett negativt beslut fattas på grundval av en bakgrundskontroll. Även om detta regelverk inte är tillämpligt i Sverige visar det på en rättssäkerhetsprincip som är förenlig med svenska och europeiska rättstraditioner.

En sådan process står även i god överensstämmelse med dataskyddsförordningens (GDPR) grundprinciper, särskilt kraven på korrekthet, transparens och rättvisa, men kompletterar GDPR genom att tydliggöra hur beslutsfattandet bör gå till när bakgrundskontroller används som underlag.

Bakgrundskontrollföretag har i detta sammanhang en central roll i att analysera och filtrera information så att endast uppgifter med faktisk relevans för riskbedömningen rapporteras vidare till arbetsgivaren. Uppgifter som saknar tydlig koppling till risk eller arbetsuppgifter, såsom enstaka mindre förseelser, bör i normalfallet inte rapporteras. Arbetsgivarens åtgärder bör därefter fokusera på proportionerliga beslut, exempelvis riskreducerande villkor eller, i förekommande fall, avstående från rekrytering, med dokumenterad och motiverad beslutsgrund.

2.6 Om uppgifter av relevans skulle komma fram vid en bakgrundskontroll under en pågående anställning, hur anser ni att uppgifterna bör hanteras?

Om uppgifter av relevans framkommer vid en bakgrundskontroll under en pågående anställning bör arbetsgivarens hantering i första hand inriktas på riskreducerande och proportionerliga åtgärder, snarare än omedelbara ingripande beslut. Bedömningen bör utgå från befattningens ansvar, mandat och faktiska åtkomst, samt från uppgifternas art, aktualitet och betydelse för den samlade riskbilden.

Hanteringen bör ske inom ramen för gällande arbetsrättsliga principer, där hänsyn tas till anställningens bestånd, individens ställning och möjligheten att vidta mindre ingripande åtgärder. I många fall kan alternativa skyddsåtgärder vara tillräckliga, exempelvis begränsad system- eller informationsåtkomst, ändrade arbetsuppgifter, förstärkt intern kontroll eller uppföljning. Sådana åtgärder kan minska risk utan att i onödan ingripa i anställningsförhållandet.

Om uppgifterna bedöms kunna leda till mer ingripande åtgärder bör hanteringen präglas av tydliga rättssäkerhetsgarantier. Det bör övervägas att tillämpa motsvarande processuella principer som vid rekrytering, där den anställde informeras om att uppgifter kan påverka arbetsgivarens bedömning och ges möjlighet att bemöta, förklara eller korrigera uppgifterna innan beslut fattas. Detta minskar risken för felaktiga eller oproportionerliga beslut och bidrar till ett starkt förtroende mellan arbetsgivare och arbetstagare.

Bakgrundskontroller under anställning bör inte användas som generella eller kontinuerliga masskontroller. De bör i stället vara kopplade till tydligt identifierade behov, såsom förändrade arbetsuppgifter, befordran, utökad åtkomst, särskilda händelser eller incidenter. Uppgifter som saknar tydlig koppling till risk eller arbetsuppgifter, exempelvis enstaka mindre förseelser, bör inte ligga till grund för åtgärder.

Bakgrundskontrollföretag har även i detta sammanhang en viktig roll i att analysera och filtrera information, så att endast uppgifter med faktisk relevans för riskbedömningen rapporteras vidare. Detta bidrar till att hanteringen förblir proportionerlig, rättssäker och förenlig med både arbetsrättsliga och dataskyddsrättsliga principer.

2.7 Ser ni några hinder mot eller problem med att göra ändamålsenliga bakgrundskontroller i dag? I så fall vilka?

Ja. Det finns i dag betydande hinder för att genomföra ändamålsenliga, rättssäkra och proportionerliga bakgrundskontroller, trots att behovet är väl identifierat i både offentlig och privat sektor.

Det mest centrala hindret rör arbetsgivares rätt att ta del av information om lagöverträdelse, även när det finns ett tydligt och legitimt behov kopplat till befattningens ansvar, mandat och skyddsvärde. Rättsläget kring behandling av sådana uppgifter enligt dataskyddsförordningens artikel 10 upplevs som otydligt och fragmenterat. I praktiken innebär detta att bakgrundskontrollföretag i vissa fall kan ha tillstånd att behandla uppgifter, medan arbetsgivare samtidigt saknar möjlighet att ta del av informationen på ett transparent, dokumenterbart och rättssäkert sätt.

Den nuvarande ordningen leder ofta till muntlig återrapportering, informella lösningar eller till att kontroller helt uteblir trots identifierade risker. Detta försvårar spårbarhet, dokumentation och likvärdig tillämpning, och kan i praktiken innebära ett svagare integritetsskydd än vid en tydligt reglerad modell.

Ett närliggande problem är den bristande och inkonsekventa tillgången till rättsdata och annan riskrelevant samhällsinformation. I avsaknad av reglerad åtkomst tvingas arbetsgivare och bakgrundskontrollföretag till manuella, tidskrävande och lokalt varierande processer, exempelvis vid inhämtning av domar och andra rättshandlingar. Detta skapar skillnader i tillämpning mellan olika verksamheter och kommuner och försvårar ett likvärdigt skydd av samhällsviktiga funktioner.

En särskilt central aspekt i detta sammanhang är tillgången till fullständiga domstolshandlingar. Sådan tillgång är av avgörande betydelse för att möjliggöra en rättssäker och proportionerlig bedömning i det enskilda fallet. Ett belastningsregisterutdrag återger i regel endast brottsrubricering och ger därmed inte tillräckligt underlag för att förstå omständigheterna kring gärningen.

Genom att ta del av domskäl och den rättsliga kontexten, inklusive eventuella förmildrande omständigheter, kan en professionell och nyanserad riskbedömning göras. I vissa fall framgår då att en lagöverträdelse saknar relevans för den aktuella befattningen eller uppdraget, trots att den i ett förenklat registerutdrag annars skulle kunna uppfattas som diskvalificerande. Tillgång till fullständiga domstolshandlingar stärker därmed både träffsäkerheten i riskbedömningen och den enskildes rättssäkerhet, samt förbättrar den granskades möjligheter att på ett rättvist sätt delta på arbetsmarknaden och, där så är relevant, återetablera sig i arbetslivet.

Samtidigt är det viktigt att understryka att fullständig tillgång till domstolshandlingar inte innebär att hela innehållet bör göras tillgängligt för arbetsgivaren. Domstolshandlingar kan innehålla omfattande och känslig information som saknar relevans för den aktuella befattningen eller uppdraget, och som inte bör ligga till grund för arbetsgivarens beslut.

Här har professionella bakgrundskontrollföretag en central och skyddande funktion. Genom att ta del av domstolshandlingar i sin helhet kan en kvalificerad relevans- och proportionalitetsbedömning göras, där endast de delar som har faktisk betydelse för riskbedömningen rapporteras vidare. Detta minskar risken för överexponering av personuppgifter, motverkar schablonmässiga bedömningar och stärker både integritetsskyddet och rättssäkerheten. En sådan ordning ligger i linje med dataskyddsförordningens principer om dataminimering och

ändamålsbegränsning och tydliggör skillnaden mellan åtkomst för analys och information som utgör beslutsunderlag.

Därtill finns en tydlig paradox mellan ansvar och verktyg. Arbetsgivare har i många fall uttryckliga skyldigheter att förebygga risker, exempelvis att säkerställa rätt att arbeta, motverka ekonomisk brottslighet, skydda barn och andra utsatta grupper eller förebygga insiderproblematik. Samtidigt saknas i dag effektiva, rättssäkra och proportionerliga verktyg för att verifiera grundläggande förhållanden såsom medborgarskap, behörigheter, legitimationer eller ekonomisk sårbarhet.

Den nuvarande otydligheten riskerar även att gynna oseriösa aktörer som saknar juridisk kompetens, metodik och informationssäkerhet, medan seriösa aktörer avstår från kontroller eller begränsar dem av rättsliga skäl. Detta snedvrider konkurrensen och försvagar integritetsskyddet i praktiken.

Mot denna bakgrund ser BKF ett tydligt behov av en sammanhållen och reglerad modell som kombinerar:

- ackreditering eller tillstånd för professionella bakgrundskontrollföretag, med tydliga krav på metodik, proportionalitet, informationssäkerhet och tillsyn,
- tydlig reglering av arbetsgivares rätt att ta del av riskrelevant information via sådana aktörer när legitimt behov föreligger, samt
- kontrollerad, loggad och spårbar åtkomst till vissa utvalda uppgifter från tillförlitliga primärkällor, inklusive domstolshandlingar, i likhet med modeller som redan används inom andra reglerade sektorer såsom bank, försäkring och kreditupplysning.

BKF vill här tydliggöra att arbetet med att ta fram en ackrediterad branschkod för bakgrundskontrollföretag inte är ett teoretiskt förslag, utan ett pågående arbete som bedrivits sedan 2024. Arbetet sker i nära dialog med Integritetsskyddsmyndigheten (IMY) och omfattar bland annat krav på metodik, proportionalitet, dataminimering, informationssäkerhet, spårbarhet och tillsyn.

BKF har som uttalad ambition att under första halvan av 2026 kunna lämna in ett första formellt underlag för ackreditering. Arbetet syftar till att skapa praktiskt tillämpbara och rättssäkra ramar för professionella bakgrundskontroller, som kan fungera som ett komplement till lagstiftning och bidra till en mer enhetlig och förutsebar tillämpning på området.

En sådan modell skulle stärka rättssäkerhet och integritet, minska behovet av informella lösningar och skapa förutsättningar för likvärdig och proportionerlig riskhantering i hela samhället.

3. Kartläggning av behovet av bakgrundskontroller i andra situationer än vid anställning, t.ex. vid ingående/uppföljning av avtal

3.1 Finns det behov att göra bakgrundskontroller i andra situationer än vid anställning?

Ja. Det finns ett tydligt och ökande behov av bakgrundskontroller även i andra situationer än vid anställning. I många verksamheter uppstår i dag betydande risker genom affärsrelationer, leverantörsled, samarbeten och andra avtalsförhållanden, snarare än genom direkta anställningar.

Genom sådana relationer kan individer och företag få åtkomst till system, information, fysiska miljöer eller möjlighet att påverka beslut och processer, utan att omfattas av traditionella rekryterings- eller säkerhetsprövningsprocesser. Detta gäller i både offentlig och privat sektor och i samtliga branscher.

Bakgrundskontroller i dessa situationer är därför ett viktigt förebyggande verktyg för att minska risken för infiltration, insiderproblematik, bedrägerier, ekonomisk brottslighet, kopplingar till organiserad brottslighet samt annan otillbörlig påverkan. Behovet förstärks av att hotaktörer i ökande grad utnyttjar legitima affärsrelationer som angreppsväg, snarare än direkta angrepp mot organisationen.

Behovet är branschöverskridande och uppstår oavsett om relationen gäller leverantörer, konsulter, bemanning, partnerskap, investeringar eller andra samarbetsformer. Avgörande är inte relationens form, utan vilken faktisk åtkomst, påverkan och vilket skyddsvärde relationen medför.

3.2 I vilka situationer finns ett sådant behov? I vilka verksamheter/situationer finns ett särskilt stort behov? Vilka potentiella risker bedöms bakgrundskontroller kunna förhindra?

Behovet av bakgrundskontroller är särskilt stort i situationer där affärsrelationer, avtal eller samarbeten medför faktisk åtkomst, beroenden eller möjlighet till påverkan på verksamheten. Det gäller oavsett om relationen avser leverantörer, konsulter, bemanningsföretag, partnerskap, investeringar eller andra samarbetsformer.

Särskilt tydligt är behovet i verksamheter och situationer där relationen innebär tillgång till ekonomiska flöden, system och it-miljöer, känslig information, fysiska miljöer eller möjlighet att påverka upphandlingar, strategiska beslut eller myndighetsutövning. Exempel på sådana situationer är upphandling och leverantörsval, outsourcing och it-drift, fastighets- och driftstjänster, strategiska samarbeten, större investeringar samt företagsförvärv.

Behovet förekommer i samtliga branscher, både inom offentlig och privat sektor, men tar sig olika uttryck beroende på verksamhetens art. Inom samhällsviktiga funktioner och offentlig verksamhet är riskerna ofta kopplade till förtroende, kontinuitet och skydd av allmänna intressen. Inom industri, teknik och fastighet kan riskerna vara kopplade till sabotage, insiderproblematik eller otillbörlig fysisk åtkomst. Inom finansiella och administrativa funktioner är riskerna ofta kopplade till ekonomisk brottslighet, bedrägerier och intressekonflikter. Gemensamt är att riskerna inte är hypotetiska, utan väl dokumenterade i medlemsföretagens kundärenden.

Bakgrundskontroller i dessa situationer kan förebygga infiltration via leverantörsled, möjliggörare för organiserad brottslighet, systematiska bedrägerier, välfärdsbrott, korruption samt otillbörlig påverkan på beslut och processer. Genom att identifiera riskindikatorer i tid kan verksamheter vidta proportionerliga åtgärder innan skada uppstår, snarare än att agera reaktivt efter en incident.

3.3 Vilka typer av bakgrundskontroller finns det behov av (till exempel kontroll av vissa register eller andra åtgärder)?

Det finns behov av bakgrundskontroller som möjliggör en strukturerad och riskbaserad bedömning av både juridiska personer och nyckelpersoner i affärs- och samarbetsrelationer. Kontrollerna bör anpassas efter relationens omfattning, skyddsvärde och faktiska påverkan, snarare än genom generella eller schablonmässiga upplägg.

För juridiska personer finns behov av kontroller som belyser bolagsstruktur, ägar- och kontrollförhållanden, företrädare och firmatecknare, samt ekonomiska förhållanden och historik, i den mån detta är relevant för att identifiera risk för oegentligheter, intressekonflikter eller utnyttjande av bolagsstrukturer i brottsliga syften.

För nyckelpersoner i affärsrelationer finns behov av att, där det är proportionerligt, kunna beakta ekonomiska förhållanden, bolagsengagemang, tidigare yrkesroller och meriter, samt information om lagöverträdelser när detta har tydlig koppling till riskbilden. Sådan information är särskilt relevant för att identifiera kopplingar till organiserad brottslighet, motverka bedrägerier och förhindra att verksamheter används som brottsverktyg.

Tillgång till domstolshandlingar är i detta sammanhang central för att möjliggöra en korrekt och proportionerlig bedömning av uppgifter om lagöverträdelser. Domstolshandlingar ger den kontext som krävs för att avgöra relevans och allvar, till skillnad från förenklade registerutdrag som ofta saknar sådan information. Samtidigt bör fullständig tillgång till domstolshandlingar användas för analys, inte för direkt vidareförmedling till uppdragsgivare, utan filtreras genom professionell relevansbedömning.

Vidare finns behov av kontroll mot internationella sanktionslistor, vilket är relevant i alla affärsrelationer. Svenska verksamheter saknar i praktiken full insyn i indirekta ägarled, internationella motparter och affärsförbindelser, varför sanktionskontroller är ett nödvändigt verktyg för regelefterlevnad och riskminimering, oavsett om relationen i sig uppfattas som internationell eller inte.

Offentlig och verifierbar information, inklusive viss mediaexponering, kan i vissa fall komplettera bedömningen när den har tydlig koppling till yrkesutövning, affärsrelationen eller förtroenderisker. Sådan information bör dock alltid bedömas med försiktighet och i sitt sammanhang.

Samtliga dessa kontroller förutsätter att de genomförs av professionella bakgrundskontrollföretag med tydlig metodik för proportionalitet, dataminimering och kvalitetssäkring. Endast uppgifter med faktisk relevans för riskbedömningen bör rapporteras vidare, medan information som saknar betydelse för relationens riskprofil bör sorteras bort.

3.4 Vilka omständigheter i situationen avgör om ett behov föreligger, exempelvis bransch, avtalspart, avtalets föremål eller värde?

Avgörande för om behov av bakgrundskontroll föreligger är relationens faktiska risk och skyddsvärde, snarare än enbart bransch, organisationsform eller avtalstyp. Bedömningen bör utgå från vilken åtkomst, påverkan eller beslutskompetens som avtalsparten eller dess företrädare får i praktiken.

Centrala omständigheter är avtalets omfattning, varaktighet och ekonomiska värde, samt om relationen innebär tillgång till ekonomiska flöden, system och it-miljöer, känslig information, fysiska miljöer eller möjlighet att påverka upphandlingar eller strategiska beslut. Även användning

av underleverantörer, komplexa ägar- eller leverantörsled samt möjligheten att byta företrädare under avtalstiden kan påverka riskbilden.

Bransch kan vara en relevant faktor i den övergripande riskbedömningen, men bör inte ensamt vara styrande. Motsvarande risker kan förekomma i många olika sektorer, medan vissa verksamheter inom samma bransch kan ha mycket olika skyddsvärde. Bedömningen bör därför vara individuell, riskbaserad och proportionerlig, och tillämpas konsekvent i både offentlig och privat sektor.

3.5 Finns det en skyldighet för verksamheten att göra sådana kontroller? Är en sådan skyldighet avtalad eller framgår den av befintliga författningar? I så fall vilka författningar?

I dag följer skyldigheter att genomföra bakgrundskontroller i andra situationer än vid anställning endast i begränsad och sektorsspecifik omfattning. Någon generell och sammanhållen skyldighet att genomföra bakgrundskontroller i affärs- och avtalsrelationer finns inte.

I vissa verksamheter följer dock krav eller förväntningar av befintlig lagstiftning eller tillsynsramar. Exempelvis kan skyldigheter att kontrollera affärspartners och företrädare följa av regelverk inom områden som upphandling, penningtvätt och finansiering av terrorism, säkerhetsskydd, samt andra regelverk som ställer krav på riskbedömning och kontroll av motparter. I dessa fall är bakgrundskontroller ett sätt att uppfylla krav på aktsamhet, riskhantering och efterlevnad, även om de inte alltid uttryckligen regleras som just bakgrundskontroller.

Utöver lagstadgade krav regleras bakgrundskontroller i många fall genom avtal. Det är vanligt att upphandlingsunderlag, samarbetsavtal och leverantörsvillkor innehåller krav på att leverantörer, konsulter eller andra parter ska uppfylla vissa integritets-, säkerhets- eller efterlevnadskrav, vilket i praktiken förutsätter någon form av bakgrundskontroll. Sådana avtalskrav varierar dock kraftigt i utformning och tillämpning.

Avsaknaden av ett tydligt och enhetligt regelverk innebär att skyldigheten att genomföra bakgrundskontroller i dag tillämpas ojämnt mellan olika sektorer och verksamheter. Detta skapar rättsosäkerhet och skillnader i skyddsnivå, samt försvårar för verksamheter att avgöra när och hur kontroller bör genomföras på ett proportionerligt och rättssäkert sätt.

3.6 Vilka uppgifter är relevanta att undersöka i en sådan bakgrundskontroll? Ge gärna exempel på olika typer av problematiska omständigheter som skulle kunna komma fram.

Relevanta uppgifter att undersöka i bakgrundskontroller av affärs- och avtalsrelationer är sådana som belyser risken att relationen kan utnyttjas för brottsliga, otillbörliga eller förtroendeskadliga syften. Bedömningen bör vara riskbaserad och anpassad till relationens omfattning, skyddsvärde och faktiska påverkan.

För juridiska personer är uppgifter om bolagsstruktur, ägar- och kontrollförhållanden, företrädare och firmateknare centrala för att identifiera dolda beroenden, bulvanupplägg eller möjligheter att kringgå ansvar. Ekonomiska förhållanden och historik kan indikera sårbarhet, finansiell instabilitet eller mönster av oegentligheter.

För nyckelpersoner i affärsrelationer kan uppgifter om ekonomiska förhållanden och betalningsförseelser vara relevanta som sårbarhetsindikatorer. Bolagsengagemang och tidigare uppdrag kan belysa intressekonflikter eller möjligheten att agera genom externa strukturer. Tidigare yrkesroller och meriter är relevanta för att bedöma faktisk erfarenhet, ansvarsnivå och tillförlitlighet.

Uppgifter om lagöverträdelser är relevanta när de har tydlig koppling till relationens riskprofil, exempelvis för att identifiera kopplingar till organiserad brottslighet, motverka bedrägerier eller förhindra att verksamheter används som brottsverktyg. I dessa fall är tillgång till domstolshandlingar särskilt viktig för att kunna bedöma relevans, allvar och aktualitet, eftersom förenklade registerutdrag ofta saknar nödvändig kontext.

Vidare är kontroll mot internationella sanktionslistor relevant i alla affärsrelationer, oavsett om relationen uppfattas som internationell eller inte. Svenska verksamheter saknar i praktiken full insyn i indirekta ägarled och affärsförbindelser, vilket gör sanktionskontroller till ett grundläggande verktyg för riskminimering och regelefterlevnad.

Problematiske omständigheter som kan framkomma är exempelvis mönster av ekonomisk misskötsamhet, återkommande bolagsengagemang i konkurser eller oegentligheter, kopplingar till organiserad brottslighet, bristande överensstämmelse mellan uppgivna meriter och verifierbar information, eller tidigare lagöverträdelser som är relevanta för relationens riskprofil.

Samtliga uppgifter bör analyseras och filtreras av professionella bakgrundskontrollföretag, så att endast information med faktisk betydelse för riskbedömningen rapporteras vidare. Uppgifter som saknar tydlig koppling till risk eller relationens skyddsvärde bör inte ligga till grund för åtgärder.

3.7 Om uppgifter av relevans skulle komma fram vid en sådan bakgrundskontroll, hur anser ni att uppgifterna bör hanteras? Med "hanteras" avses inte eventuell personuppgiftsbehandling, utan kontrollantens faktiska agerande efter kännedom om uppgiften.

Om uppgifter av relevans framkommer vid bakgrundskontroller i affärs- och avtalsrelationer bör hanteringen utgå från en riskbaserad och proportionerlig bedömning, där uppgifternas betydelse vägs mot relationens omfattning, skyddsvärde och faktiska påverkan på verksamheten. Uppgifterna bör inte leda till automatiska eller schablonmässiga beslut, utan användas som ett underlag för välavvägda riskmitigerande åtgärder.

Hanteringen bör fokusera på framåtblickande riskreduktion, exempelvis genom avtalsvillkor, begränsad åtkomst, förstärkt uppföljning, särskilda kontrollmekanismer eller i vissa fall avstående från att ingå eller fortsätta relationen. Vilken åtgärd som är lämplig bör avgöras av uppgifternas art, aktualitet och relevans för den aktuella relationen.

Professionella bakgrundskontrollföretag har här en central funktion i att analysera, värdera och filtrera information, så att endast uppgifter med faktisk betydelse för riskbedömningen rapporteras vidare. Uppgifter som saknar tydlig koppling till risk eller relationens skyddsvärde, såsom enstaka mindre förseelser eller information utan relevans för uppdraget, bör i normalfallet inte ligga till grund för beslut och bör inte rapporteras.

När uppgifter kan få betydande konsekvenser för relationen bör hanteringen präglas av rättssäkerhet och transparens. Det kan i vissa fall vara lämpligt att ge berörd part möjlighet att lämna förklaringar eller kompletterande information, särskilt när uppgifterna är komplexa eller kräver kontext för att bedömas korrekt. Detta bidrar till mer träffsäkra bedömningar och minskar risken för oproportionerliga beslut.

Sammantaget bör hanteringen av uppgifter syfta till att möjliggöra proportionerliga och dokumenterade beslut, där både verksamhetens skyddsintresse och den berörda partens rättssäkerhet beaktas.

3.8 Ser ni några hinder mot eller problem med att göra ändamålsenliga bakgrundskontroller i dag? I så fall vilka?

Ja. I huvudsak är hindren desamma som vid bakgrundskontroller inför och under anställning, men får i affärs- och avtalsrelationer ofta ännu större praktisk betydelse, eftersom relationerna kan vara komplexa, långvariga och omfatta flera nivåer av företrädare och underleverantörer.

Ett centralt hinder är den otydliga regleringen av tillgång till information om lagöverträdelse, särskilt i relation till nyckelpersoner hos avtalspartners. Även när ett legitimt behov föreligger saknas ofta tydliga och rättssäkra möjligheter att ta del av riskrelevant information på ett strukturerat och dokumenterbart sätt. Detta försvårar konsekventa bedömningar och leder i praktiken till att kontroller genomförs ad hoc eller inte alls.

Vidare är tillgången till rättsdata, inklusive domstolshandlingar, bristfällig och fragmenterad. Detta försvårar proportionerliga bedömningar av relevans och allvar vid uppgifter om lagöverträdelse och ökar risken för antingen överdrivet försiktiga eller otillräckliga åtgärder. Utan tillgång till rätt kontext riskerar bedömningarna att bli schablonmässiga, vilket varken gynnar rättssäkerheten eller verksamhetens riskhantering.

Ett ytterligare problem är att affärsrelationer ofta omfattar indirekta ägar- och kontrollled, där svenska verksamheter saknar insyn utan tillgång till tillförlitliga primärkällor och strukturerade analyser. Detta försvårar arbetet med att identifiera kopplingar till organiserad brottslighet, ekonomisk brottslighet eller sanktionsöverträdelse.

Slutligen innebär avsaknaden av en sammanhållen och reglerad modell att tillämpningen varierar kraftigt mellan verksamheter och sektorer. Detta skapar rättsosäkerhet och snedvrider konkurrensen. En ordning som kombinerar ackrediterade bakgrundskontrollföretag, tydliga ramar för tillgång till riskrelevant information samt kontrollerad, loggad och spårbar åtkomst till utvalda primärkällor skulle avsevärt förbättra möjligheterna att genomföra ändamålsenliga, proportionerliga och rättssäkra bakgrundskontroller även i dessa situationer.

Mot bakgrund av ovanstående vill BKF uppmana utredningen att i det fortsatta arbetet föra en fördjupad dialog med branschen. BKF bidrar gärna som samtalspartner i frågor som rör praktisk tillämpning, proportionalitetsbedömningar och hur en framtida reglering kan utformas för att samtidigt stärka integritetsskydd, rättssäkerhet och skyddet för samhällsviktiga verksamheter

Vänliga hälsningar,

Johan Söderström
Ordförande, Bakgrundskontrollföretagen (BKF)

PrimeSafe
ToFindOut
2Secure
Tempest Risk Solution
Valida
SRS Security
Validata
Nordic LEVEL Group
Recway