FSPOS

Medarbetarsäkerhet inom finansiell sektor

FSPOS AG Analys

2024-06-17

Sammanfattning

Hoten mot den finansiella sektorn har ökat på flera fronter och hot finns i bredden av sektorns verksamhet. Bland annat har hotet från möjliggörare, individer som nyttjar sin ställning i en verksamhet för att exempelvis stötta organisad brottslighet, ökat. Den ökade hotbilden ställer högre krav på säkerhetsarbetet inom den finansiella sektorn i sin helhet. En viktig aspekt i en verksamhets säkerhet är medarbetarna, vilka kan vara både en styrka och en sårbarhet i säkerhetsarbetet. Alla som deltar i en verksamhet och därmed har information om, eller möjlighet att påverka verksamheten, kan utgöra en risk. Säkerhetsarbetet inom en verksamhet bör därför innefatta arbete med säkerhetsfrågor relaterade till medarbetare.

Denna promemoria syftar till att redogöra för hur den finansiella sektorns aktörer kan arbeta med säkerhetsfrågor relaterade till medarbetare. Det är frågor som: lojalitet, pålitlighet och kunskap om säkerhet. I promemorian har begreppet *medarbetarsäkerhet* använts för åtgärder relaterat till medarbetare inom icke säkerhetskänslig verksamhet. Begreppet används för att hålla isär dessa åtgärder från de åtgärder som är lagstadgade inom *personalsäkerhet,* det vill säga åtgärder inom säkerhetskänslig verksamhet som ska genomföras enligt säkerhetsskyddslagen (2018:585). För åtgärder inom medarbetarsäkerhet finns inte samma entydiga kravbild och inte heller samma typ av lagstöd för att genomföra vissa åtgärder.

I promemorian exemplifieras var krav på finansiella aktörers arbete med medarbetarsäkerhet ställs, vilka åtgärder som kan genomföras och viktiga aspekter, såsom arbetsrätt och personlig integritet, som måste beaktas då arbetet med medarbetarsäkerhet utformas. Följande åtgärder, fördelade på perioderna före, under och vid avslut av en medarbetares anställning, presenteras inom området medarbetarsäkerhet:

- **Före anställning:** interna riktlinjer, policyer och dokument, bakgrundskontroll, drogtest samt avtalssignering
- **Under anställning:** utbildning, tillträdes- och behörighetsbegränsning, rapporteringsvägar, uppföljande samtal, rotering och fyra-ögonsprincipen samt återkommande drogtester
- **Vid avslut av anställning:** återlämning av material och utrustning samt avslutningssamtal

Åtgärderna bör även nyttjas för leverantörer som deltar i verksamheten, både på plats och i egna lokaler. Vilka åtgärder som bör används och till vilken omfattning bör baseras på verksamhetens riskanalys. För åtgärder som är integritetskänsliga, vilket även gäller åtgärderna säkerhetsprövning och registerkontroll inom personalsäkerhet, är det mycket viktigt att säkerställa att den personliga integriteten vägs mot det berättigade intresset för kontrollerna.

Arbetet med medarbetarsäkerhet spänner över en organisations hela verksamhet och för de som arbetar inom säkerhetskänslig verksamhet kompletteras medarbetarsäkerhet med åtgärder inom personalsäkerhet. Arbetet avser att skydda verksamheten från medarbetarna men syftar även till att skydda medarbetarna från externa påtryckningar samt till att stärka säkerhetskulturen. En viktig del av arbetet med medarbetarsäkerhet är att komma ihåg att medarbetarna är en av verksamhetens viktigaste tillgångar, både i säkerhetsarbetet och i stort.

Innehåll

1 Inledning

Det säkerhetspolitiska läget i Europa har under de senaste åren försämrats, där Rysslands invasion av Ukraina 2022 särskilt har gjort avtryck. Det är tydligt att det säkerhetspolitiska läget har fått följder även för Sverige. I sitt tal på Folk och Försvars Rikskonferens i januari 2024 uttryckte ministern för civilt försvar, Carl- Oscar Bohlin, att: ”Världen möter en säkerhetspolitisk utveckling med större risker än sedan andra världskrigets slut”[1] och det tydliggjordes att aktivt medvetandegörande kring säkerhet står högt på agendan för Sverige.

I Säkerhetspolisens årsbok 2023–2024[2] beskrivs hotbilden som komplex och att läget bidrar till en växande extremism och ett ökat attentatshot. Med utgångspunkt i det allvarliga omvärldsläget betonar Säkerhetspolisen vikten av att skydda verksamhet av betydelse för Sveriges säkerhet eller som omfattas av ett för Sverige förpliktande internationellt åtagande om säkerhetsskydd, härefter *säkerhetskänslig verksamhet*, och samhällsviktiga funktioner inom flera sektorer. En av de sektorer som framhävs är den finansiella sektorn, och från den Svenska Bankföreningen konstateras att ”säkerhet är en grundförutsättning för bankverksamhet”[3] och att säkerhetsarbetet under senare år har intensifierats.

Hotbilden mot den finansiella sektorn har ökat på flera fronter. Hoten kommer delvis från främmande makt, men även från organiserad brottslighet. Detta ställer högre krav på ett allomfattande säkerhetsarbete för sektorn i sin helhet, inte bara för bankerna. Risker och hot mot den finansiella sektorn finns i bredden av verksamheten i områden som: informations- och cybersäkerhetsområdet, bedrägerier och finansiell brottslighet, samt penningtvätt där det även finns risk för finansiering av terrorism.[4] Även hot från så kallade *möjliggörare* förekommer inom den finansiella sektorn.

En möjliggörare är en anställd individ som nyttjar sin ställning inom en legal verksamhet för att exempelvis stötta organisad brottslighet så som kriminella nätverk, men även egna ekonomiska intressen eller missnöje mot verksamheten kan vara drivkrafter för att agera möjliggörare. I en studie genomförd av Brottsförebyggande rådet (2024)[5] beskrivs att möjliggörare framför allt agerar förmedlare av information. Möjliggörare uppges även bistå kriminella nätverk i aktiviteter som penningtvätt och bedrägerier inom bank och finans. Möjliggörare kan agera genom att medvetet fatta felaktiga beslut eller lämna ut personuppgifter som får följder för verksamhetens förmåga att utföra sitt uppdrag genom åsamkandet av till exempel ekonomiska eller förtroenderelaterade konsekvenser.[6]

En viktig aspekt i en verksamhets säkerhet är således medarbetarna, vilka kan vara både en styrka och en sårbarhet för säkerheten. Alla personer som deltar i en verksamhet och därmed har information om, eller möjlighet att påverka verksamheten, kan utgöra en risk. Säkerhetsarbetet inom en verksamhet bör därför innefatta arbete med säkerhetsfrågor relaterade till medarbetare.

---

[1] *Anförande av Carl-Oskar Bohlin, minister för civilt försvar, vid Folk och Försvars Rikskonferens 2024.*

[2] *Säkerhetspolisen, (2024). Lägesbild 2023–2024.*

[3] *Svenska Bankföreningen, (2023). Säkerhet. Hämtad: 2024-02-20.*

[4] *Svenska Bankföreningen, (2024). Hotbildsbedömning för Sveriges Banker.*

[5] *BRÅ, (2024). Möjliggörare för kriminella nätverk - Om möjliggörare i kommunal, statlig och privat sektor. Rapport 2024:2.*

[6] *Ibid.*

Detta arbete kan innebära åtgärder för att skapa eller stärka en säkerhetskultur där det säkerställs att medarbetare har tillräcklig kunskap om, och förståelse för, verksamhetens hotbild och vidtagna säkerhetsåtgärder. Det kan även innebära åtgärder för att säkerställa att medarbetare är lojala och pålitliga, samt att de inte har sårbarheter som kan nyttjas för påtryckning. Syftet med arbetet är att minimera det hot som de egna medarbetarna kan utgöra för en verksamhet samt att stärka medarbetarnas förståelse för säkerhetsfrågor och bygga en stark säkerhetskultur.

Inom säkerhetskänslig verksamhet ska säkerhetsfrågor relaterade till bland annat medarbetares lojalitet, pålitlighet och kunskap om säkerhet, hanteras enligt personalsäkerhet inom ramen för säkerhetsskyddslagen (2018:585).[7] För motsvarande frågor inom icke säkerhetskänslig verksamhet finns idag inte samma entydiga lagstiftning att ta stöd i när behov finns att utreda en medarbetares lojalitet och pålitlighet. Detta kan dock komma att ändras; SOU 2019:19 *Belastningsregisterkontroll i arbetslivet*[8] pekar på ett behov av författningsstöd för att framgent kunna bakgrundskontrollera viss personal inom den finansiella sektorn. Även för de verksamheter som omfattas av det så kallade CER-direktivet pågår en utredning om hur bakgrundskontroller enligt direktivet ska kunna genomföras.[9,10] Utöver detta skickade Integritetsmyndigheten i juni 2024 en hemställan till regeringen om att utreda förutsättningar för bakgrundskontroller i syfte att lämna nödvändiga författningsförslag där behovet av kontroller balanseras med skyddet för den personliga integriteten.[11]

Krav ställs dock på aktörer inom finansiell sektor att säkerställa att personal inom verksamheten är lämpliga ur ett säkerhetsperspektiv. Därför finns ett behov av att beskriva hur arbete med säkerhetsfrågor relaterade till medarbetare kan hanteras inom den finansiella sektorn, detta specifikt avseende medarbetare inom icke säkerhetskänslig verksamhet. Arbetet med säkerhetsfrågor relaterade till medarbetare behöver utformas utifrån den specifika verksamheten, de hot som föreligger, samt gällande lagstiftning. Denna promemoria kommer att analysera hur verksamheter inom den finansiella sektorn kan arbeta med just detta.

1.1 Syfte och mål

Denna promemoria syftar till att redogöra för hur den finansiella sektorns aktörer kan arbeta med säkerhetsfrågor relaterade till medarbetare; ett område som blir viktigare då kriminella nätverk alltmer intresserar sig för att rekrytera eller placera möjliggörare inom sektorns verksamheter, samtidigt som det säkerhetspolitiska läget innebär ökat intresse från främmande makt att infiltrera säkerhetskänslig verksamhet.

Denna promemoria avser att ge exempel på åtgärder som kan användas i arbetet med säkerhetsfrågor relaterade till medarbetare, samt analysera tillämpningen av dessa åtgärder och de eventuella arbetsrättsliga aspekter som kan påverka tillämpningen. Denna promemoria avser även att redogöra för skillnader i arbetet mellan de verksamheter som omfattas av och de som inte omfattas av säkerhetsskyddslagen.

---

[7] *SFS 2018:585 Säkerhetsskyddslag.*

[8] *SOU 2019:19 Belastningsregisterkontroll i arbetslivet - behovet av utökat författningsstöd.*

[9] *Dir. 2023:30 Genomförande av EU:s direktiv om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen och EU:s direktiv om kritiska entiteters motståndskraft.*

[10] *Dir. 2022/2557 Europaparlamentets och rådets direktiv (EU) 2022/2557 av den 14 december 2022 om kritiska entiteters motståndskraft och om upphävande av rådets direktiv 2008/114/EG.*

[11] *Integritetsmyndigheten (2024). Hemställan om utredning avseende bakgrundskontroller, IMY-2024-8036*

Målet med denna promemoria är att ge aktörer inom den finansiella sektorn en ökad förmåga i arbetet med säkerhetsfrågor kopplade till medarbetare.

1.2 Genomförande

Underlaget till denna promemoria utgörs av två huvudsakliga källtyper. Innehållet bygger på skriftliga underlag med fokus på hotbilden mot den finansiella sektorn och medarbetarens roll i en säker verksamhet, så som rapporter från: Säkerhetspolisen, Svenska Bankföreningen och Brottsförebyggande rådet (Brå). Utöver detta har lagtext och riktlinjer relaterat till bland annat Säkerhetsskyddslagen (2018:585), Regeringsreformen (1974:152) och Dataskyddsförordningen (GDPR) använts. Innehållet baseras även på diskussioner inom en referensgrupp bestående av representanter från olika delar av den finansiella sektorn. Referensgruppen har bistått med praktiska erfarenheter av, och kunskap om, säkerhetsarbete inom sektorn, samt bistått med synpunkter på hur promemorian ska bli så relevant som möjligt för aktörerna i finansiell sektor. Allt insamlat underlag, både det skriftliga underlaget samt inhämtad information från referensgruppen, har analyserats och sammanställts i denna promemoria.

1.3 Avgränsning

Alla verksamheter har materiella och immateriella värden som behöver skyddas.[12] Detta görs inom ramen för en verksamhets övergripande säkerhetsarbete som syftar till att värna och trygga dessa värden och därigenom säkerställa verksamhetens förmåga att utföra sitt uppdrag. Termen säkerhetsarbete är ett brett begrepp vars innebörd kan variera beroende på verksamhet. Inom ramen för denna promemoria kommer säkerhetsrelaterade aspekter som berör skydd för verksamheten mot illojala handlingar från medarbetare, samt en stärkt säkerhetskultur som främjar medarbetares kunskap och engagemang i säkerhetsfrågor att diskuteras.

Figur 1. Medarbetarsäkerhet som en del av det övergripande säkerhetsarbetet.

Idag finns inget vedertaget begrepp som behandlar säkerhetsfrågor kopplat till medarbetare utanför säkerhetskänslig verksamhet. Inom säkerhetskänslig verksamhet, enligt säkerhetsskyddslagen (2018:585), används begreppet *personalsäkerhet*. För att förtydliga avgränsningen av säkerhetsfrågor i denna promemoria så kommer begreppet *medarbetarsäkerhet* användas för motsvarande frågor inom icke säkerhetskänslig verksamhet. Diskussion om personalsäkerhet inom säkerhetskänslig verksamhet återfinns i kapitel *Särskilda krav på säkerhetskänslig verksamhet*.

Begreppet medarbetarsäkerhet syftar i denna promemoria till den del av en verksamhets övergripande säkerhetsarbete som kopplas till medarbetare. Åtgärder inom medarbetarsäkerhet är dels specifikt utformade för att skydda verksamheten mot de hot medarbetare kan utgöra. Här åsyftas hot i form av illojala medarbetare som exempelvis möjliggörare, men även det hot och

[12] *Försvarsmakten, (2021). Reglemente Säkerhetstjänst.*

sårbarheter som bristande kunskap i säkerhetsfrågor hos medarbetarna kan utgöra. Medarbetarsäkerhet syftar också till att stärka medarbetarnas kunskap om och förståelse för säkerhetsfrågor och därmed även stärka den del av skyddet som medarbetarna formar.

Denna promemoria avgränsas till att inte beröra Finansinspektionens ledningsprövning[13], vilket avser en lämplighetsbedömning av ledningen inom finansiella företag. En ytterligare avgränsning som görs är att personsäkerhet, det vill säga personlig säkerhet med syfte att säkerställa en medarbetares trygghet i vardagen, inte berörs i denna promemoria. Personsäkerhet är en viktig del inom säkerhetsarbetet i en verksamhet. Personer med specifika tjänster eller personer som skulle kunna hamna i riskfyllda situationer kan vara i behov av personlig säkerhet, en analys som bör göras i verksamhetens hot- och riskanalys.

1.4 Läsanvisning

För att redogöra hur aktörer inom den finansiella sektorn kan arbeta med säkerhetsfrågor relaterade till medarbetare inom både säkerhetskänslig verksamhet och icke säkerhetskänslig verksamhet har denna promemoria strukturerats i sex kapitel. Kapitel 1–4 fokuserar enbart på säkerhetsfrågor relaterade till medarbetare i icke säkerhetskänslig verksamhet. Kapitel 5 behandlar säkerhetskänslig verksamhet.

I kapitel 2 *Medarbetare som en del av hotbilden* beskrivs den del av hotbilden som medarbetare kan utgöra för en verksamhet. Utöver detta beskrivs hotet från möjliggörare inom ramen för icke säkerhetskänslig verksamhet närmare, detta med fokus på den finansiella sektorn.

I kapitel 3 *Medarbetarsäkerhet som en del av säkerhetsarbetet* beskrivs medarbetarsäkerhet som en del av det övergripande säkerhetsarbetet samt vikten av en stark säkerhetskultur.

I kapitel 4 *Arbete med medarbetarsäkerhet* presenteras och analyseras åtgärder som kan vidtas i icke säkerhetskänslig verksamhet inom ramen för medarbetarsäkerhet.

I kapitel 5 *Särskilda krav på säkerhetskänslig verksamhet* presenteras särskilda krav för säkerhetskänslig verksamhet, och personalsäkerhet sätts i relation till medarbetarsäkerhet.

Det sista kapitlet, kapitel 6 *Avslutande reflektioner*, innehåller en avslutande reflektion och sammanfattning av promemorian.

2 Medarbetare som en del av hotbilden

Medarbetarna är en av de viktigaste tillgångar en verksamhet har, både för verksamhetens framgång men också för dess säkerhet. Medarbetare kan dock också utgöra en sårbarhet för verksamheten, genom att begå misstag eller genom att medvetet använda sin ställning för att dra nytta av, eller skada, verksamheten. Risken för att medarbetare begår misstag kommer alltid finnas men kan reduceras genom exempelvis kontinuerlig utbildning. Risken för att medarbetare medvetet genomför handlingar som kan verka skadligt för verksamheten kan minskas genom åtgärder inom ramen för medarbetarsäkerhet.

[13] *Ledningsprövning genomför med stöd av bland annat lagen (2004:297) om bank- och finansieringsrörelse, lagen (2007:528) om värdepappersmarknaden och försäkringsrörelselagen (2010:2043) samt EU-förordningar om centrala motparter och transaktionsregister samt värdepapperscentraler.*

En medarbetare som medvetet använder sin position inom en verksamhet för att dra nytta av verksamheten kan göra det genom att exempelvis begå stölder eller bedrägerier, bedriva utpressning, sabotera verksamheten eller läcka information till utomstående. Detta antingen för egen vinning eller för att möjliggöra för externa parter att dra nytta av verksamheten.

2.1 Möjliggörare

Hotet från möjliggörare inom den finansiella sektorn är en kontinuerlig faktor att ta hänsyn till och att arbeta aktivt med frågor inom medarbetarsäkerhet är därför högst aktuellt.[14] De skador en möjliggörare kan åsamka en verksamhet kan vara allvarliga, i form av exempelvis läckage av känslig information och personuppgifter, påverkade beslutsprocesser, ekonomiska förluster och ett skadat förtroende eller skadande kundrelationer.

En möjliggörares vanligaste uppgift är att delge information till utomstående. Dock bedöms efterfrågan på möjliggörare som kan hantera brottsvinster ha ökat. Detta beror bland annat på samhällets arbete för att försvåra och förhindra att brottsvinster omsätts i den legala ekonomin, exempelvis genom bankers mer omfattande och rigorösa arbete mot penningtvätt.[15] Möjliggörare inom bankverksamhet kan därför vara attraktiva för kriminella nätverk. Möjliggörare inom bankverksamhet har bland annat gjort avsteg från rutiner kopplade till överföringar och godkännande av lån, hjälpt kriminella nätverk att utforma trovärdiga kreditansökningar med felaktiga inkomstuppgifter, samt möjliggjort för penningtvätt genom att dela kunskap om finansiella regleringar.[16] Det finns även exempel där annonsering skett, av bland annat kriminella nätverk, efter personer som kan vara beredda på att injicera skadlig kod i bankers IT-system.[17]

Det finns olika typer av möjliggörare, där den vanligaste typen bedöms vara de som upparbetas under anställningstiden[18]. En del möjliggörare behöver inte ens vara medvetna om sin roll, då de manipulerats till att hjälpa till. Det finns också möjliggörare som placeras i den verksamhet där de ska verka, samt affärsmässiga möjliggörare som tar betalt för sina tjänster.[19] Det är ovanligt, men förekommer, att kriminella nätverk upparbetar nya kontakter till att vara möjliggörare. Vanligare är att personer i nätverket av släkt, vänner och affärskontakter nyttjas.[20] Sociala nätverk som exempelvis LinkedIn, eller andra öppna informationsskällor, kan användas av kriminella nätverk i deras kartläggning av potentiella och lämpliga möjliggörare.[21] Manipulering är en viktig del i kriminella nätverks rekrytering av möjliggörare och sedan hålls möjliggörarna hårt, ibland under hot. Det finns således personer som agerar möjliggörare på grund av hot riktade mot medarbetaren eller dennes närstående. Att sluta som möjliggörare kan vara svårt men kan ske på olika sätt. Om möjliggöraren väljer att sluta kan det vara förknippat med ”böter” till det kriminella nätverket. Vanligt är dock att möjliggöraren blir avslöjad och tvingas ut ur den verksamhet denne verkar inom.[22]

---

[14] *Svenska Bankföreningen, (2024). Hotbildsbedömning för Sveriges Banker.*

[15] *Brå, (2024). Möjliggörare för kriminella nätverk - Om möjliggörare i kommunal, statlig och privat sektor. Rapport 2024:2.*

[16] *Ibid.*

[17] *Svenska Bankföreningen, (2024). Hotbildsbedömning för Sveriges Banker.*

[18] *Brå, (2024). Möjliggörare för kriminella nätverk - Om möjliggörare i kommunal, statlig och privat sektor. Rapport 2024:2.*

[19] *Ibid.*

[20] *Ibid.*

[21] *Svenska Bankföreningen, (2024). Hotbildsbedömning för Sveriges Banker.*

[22] *Brå, (2024). Möjliggörare för kriminella nätverk - Om möjliggörare i kommunal, statlig och privat sektor. Rapport 2024:2.*

3 Medarbetarsäkerhet som en del av säkerhetsarbetet

För att integrera medarbetarsäkerhet som en del av det övergripande säkerhetsarbetet i en verksamhet, är det viktigt att säkerhetsarbetet dimensioneras efter de värden som ska skyddas och de hot dessa värden kan stå inför. Arbetet med medarbetarsäkerhet bör grundas i ett identifierat hot mot verksamheten där medarbetare kan utgöra en sårbarhet, men det är också avhängigt vilken typ av verksamhet som bedrivs och kravbilden på verksamheten. Arbetet bör även sammanfalla med övrigt säkerhetsarbete inom en verksamhet. Skyddsåtgärder inom ramen för medarbetarsäkerhet behöver, liksom allt säkerhetsarbete, vara balanserade. För att uppnå balans bör beslut om relevanta skyddsåtgärder grunda sig i verksamhetens riskanalys där *vilka värden* som ska skyddas, och *från vad* de ska skyddas, har identifierats.

Avseende medarbetarsäkerhet finns olika perspektiv som bör beaktas i en riskanalys, till exempel medarbetarnas kunskaper om, och möjlighet att utföra sitt arbete på ett säkert sätt, samt huruvida det föreligger risk för möjliggörare i verksamheten. Riskanalysen bör ha sin utgångspunkt i vilket hot en medarbetare kan utgöra med den tillgång till information, system eller lokaler som denne har i tjänsten. Analysen bör även grundas i vilket intresse som kan finnas från exempelvis kriminella nätverk att närma sig vissa medarbetare på grund av deras tillgång till information.

Beroende på de arbetsuppgifter som ingår i olika befattningar ser tillgång till information, lokaler och IT-system olika ut, vilket innebär att hotbilden mot medarbetare kan variera. Behovet av åtgärder kommer därför också se olika ut för olika medarbetare. För att säkerställa att rätt åtgärder inom medarbetarsäkerhets vidtas, samt att rättslig grund finns för åtgärderna, kan riskanalysen kompletteras med en kartläggning av verksamhetens befattningar. Analysen bör då även ange vilka åtgärder som är relevanta för respektive befattning. En analys och kartläggning av befattningar bör regelbundet ses över för att säkerställa att analysen hålls aktuell.

3.1 Krav på medarbetarsäkerhet

Att verksamheter ska genomföra arbete som faller in under medarbetarsäkerhet finns kravställt både direkt och indirekt, exempel där denna typ av krav finns är listade i tabell 1. Listan ska inte ses som en fullständig kravlista utan som ett underlag för analys. För lagar angivna i tabell 1 kan exempelvis relevanta tillhörande föreskrifter, förordningar och riktlinjer finnas.

Verksamheter eller individer inom finansiell sektor kan välja att licensiera sig, något som ofta innebär krav på sakkunskap och kompetens men också krav kopplats till medarbetarsäkerhet såsom regelefterlevnad och god etik.

Tabell 1. Krav kopplade till området medarbetarsäkerhet inom finansiell sektor. Listan ska inte ses som en fullständig kravlista utan som ett underlag för analys.

Krav	Kort beskrivning	Relation till medarbetarsäkerhet
Arbetsmiljölag (1977:1160)	Lagens ändamål är att förebygga ohälsa och olycksfall i arbetet samt att även i övrigt uppnå en god arbetsmiljö.	Innehåller bland annat krav på att medarbetare ska ha god kännedom om de förhållanden under vilka arbetet bedrivs och vilka risker som föreligger. Lagen ställer även krav på utbildning om risker.

Lag (2018:1219) om försäkringsdistribution	Lagen innehåller bestämmelser om försäkringsdistribution som gäller för försäkringsförmedlare och -företag.	Innehåller bland annat krav kopplat till kompetens men också kopplat till att person som bedriver försäkrings-distribution inte får förekomma i det register som förs enligt lagen (1998:620) om belastningsregister avseende vissa typer av ekonomisk brottslighet.
Lag (2017:630) om åtgärder mot penningtvätt och finansiering av terrorism	Lagen syftar till att förhindra att finansiell verksamhet och annan näringsverksamhet utnyttjas för penningtvätt eller finansiering av terrorism.	Innehåller bland annat krav på rutiner för lämplighetsprövning och utbildning för anställda som deltar i verksamheten.
Finansinspektionens föreskrifter och allmänna råd om hantering av operativa risker (FFFS 2014:4)	Föreskriften innehåller bestämmelser om hur följande företag ska hantera sina operativa risker: bankaktiebolag, sparbanker, medlemsbanker, kredit-marknadsbolag, kreditmarknads-föreningar och värdepappersbolag.	Innehåller bland annat krav på rutiner för hur operativa risker kopplade till personal ska hanteras, det avser bland annat nödvändiga uppgifter om personen, eventuella intressekonflikter samt personalens kompetens.
Digital Operational Resilience Act (DORA)	DORA-förordningen syftar till att stärka den finansiella sektorns motståndskraft mot cyberrisker.	Innehåller bland annat krav kopplade till utbildning av personal kopplat till ICT-risker samt krav på hur verksamheter ska arbeta med behörighetsbegränsningar.
Directive on the resilience of critical entities (CER-direktivet)	CER-direktivet ställer krav på åtgärder för att stärka motstånds-kraften i viss samhällsviktig verksamhet. *Börjar tillämpas 18 oktober 2024.*	Innehåller krav om att bakgrundskontroller ska genomföras för personer som ingår i specifika personalkategorier.
Network and Information Security Directive (NIS2-direktivet)	NIS-direktivet syftar till att uppnå en hög gemensam nivå på säkerhet i nätverk och informationssystem inom EU. Kraven i NIS2 avser att harmonisera införlivandet av reglerna i NIS och ställer tydligare krav på bland annat riskanalyser och olika säkerhetsåtgärder. *NIS2 börjar tillämpas 18 oktober 2024.*	Innehåller krav på personalsäkerhetsåtgärder kopplade till riskhantering (så som åtkomst och tillgång) samt på utbildning inom cybersäkerhet.

3.2 *Medarbetarsäkerhet för leverantörer*

Arbetet med medarbetarsäkerhet omfattar inte bara verksamhetens egna medarbetare. Medarbetarsäkerhet omfattar även leverantörer som deltar i verksamheten, både på plats och i egna lokaler, samt leverantörer som utför annan typ av arbete i verksamhetens lokaler. Det gäller således alla leverantörer, från resurskonsulter som arbetar som en del av linjeverksamheten till leverantörer som tillhandahåller IKT-tjänster för viktiga funktioner, eller personal som ibland befinner sig i lokalerna för att utföra arbete såsom service eller underhåll. I riskanalysen bör därmed risker och åtgärder kopplade till leverantörer också analyseras.

Om åtgärder inom medarbetarsäkerhet kan bli aktuella innan leverantörens personal får tillgång till dator eller lokaler, bör detta avtalas med leverantören. Vilka åtgärder som är relevanta för leverantörers personal beror på i vilken omfattning personalen kommer att delta i verksamheten. Åtgärderna för personal från en leverantör bör vara desamma som för en av verksamhetens medarbetare som arbetar med samma information och/eller åtkomst.

Utöver att avtala med leverantören om att dennes personal kan bli föremål för åtgärder inom medarbetarsäkerhet bör krav även ställas på leverantören för att säkerställa dennes säkerhetsarbete generellt. Detta blir speciellt viktigt i de fall där exempelvis konsulter utför verksamhetens arbete i egna lokaler eller i de fall leverantörer behöver förvara information om verksamheten eller dess förhållanden.

3.3 Vikten av en stark säkerhetskultur

Medarbetare kan utgöra både en sårbarhet och en styrka för en verksamhets säkerhet. Det senare blir speciellt sant om verksamheten har en stark säkerhetskultur. Säkerhetskultur kan definieras som ”…de gemensamma värderingar, kunskaper, attityder och beteenden hos medarbetare inom en verksamhet som är inriktade på att skapa säkerhet”.[23] Säkerhetskultur omfattar således allt säkerhetsarbete och en organisations säkerhetskultur utgår från chefer och medarbetares föreställningar om säkerhet, hot och risker. Att ha en stark säkerhetskultur innebär att säkerhetsarbetet genomsyrar verksamheten och för att det ska ske är det nödvändigt att chefer och ledare har förståelse för, kunskap om och engagemang i arbetet med säkerhetsfrågor.[24] Detta för att skapa en miljö där säkerhet har en självklar plats på agendan men också för att ett nära ledarskap och en arbetsplats präglad av psykologisk trygghet är viktig för att kunna fånga upp signaler om säkerhetsbrister, sårbarheter eller möjliggörare.[25]

Att bygga en stark kultur tar tid och samma sak gäller lojalitet. Idag är rörligheten på arbetsmarknaden större än vad den tidigare varit. Medarbetare stannar inte lika länge på sina arbetsplatser, något som kan försvåra både kulturbyggande och lojalitetsbyggande. Till detta har digitalt distansarbete blivit mer vanligt förekommande, bland annat som ett resultat av Covid-19-pandemin. Distansarbete medför ett antal nya sårbarheter och hot mot verksamheter som behöver beaktas. När det kommer till hotet från möjliggörare kopplat till distansarbete är det nödvändigt att uppmärksamma det skydd som en fysisk arbetsplats, där arbete sker nära kollegor och chefer, kan utgöra samt att arbete på plats kan påverka både kultur och lojalitet positivt.[26] Ofta är det kollegor eller chef som har en viktig roll när det kommer till att upptäcka möjliggörare eller notera sårbarheter hos kollegor.[27] Det blir svårare för kollegor och chefer att till exempel lägga märke till beteendeförändringar hos en medarbetare som arbetar på distans och säkerhetskulturen riskerar att påverkas.

---

[23] *Integritetsmyndigheten, Säkerhetskultur. Hämtad: 2024-02-20.*

[24] *Ibid.*

[25] *Brå, (2024). Möjliggörare för kriminella nätverk - Om möjliggörare i kommunal, statlig och privat sektor. Rapport 2024:2.*

[26] *Ibid.*

[27] *Ibid.*

4 Arbete med medarbetarsäkerhet

Att skapa och bibehålla en stark säkerhetskultur är ett kontinuerligt arbete i en verksamhet. Arbete med medarbetarsäkerhet är en del av arbetet med säkerhet och säkerhetskultur, och inbegriper åtgärder som direkt syftar till att minska det hot medarbetare kan utgöra mot verksamheten samt åtgärder för att stärka den barriär som medarbetare också utgör i säkerheten. Åtgärder inom medarbetarsäkerhet berör således medarbetarnas pålitlighet och lojalitet, samt deras kunskap och förståelse för säkerhetsarbetet. Åtgärderna är viktiga byggstenar i skapandet av en stark säkerhetskultur.

I detta kapitel presenteras åtgärder som kan används inom den finansiella sektorn inom ramen för arbetet med medarbetarsäkerhet. Åtgärderna är avsedda att användas före, under och efter anställning. Kapitlets mål är att beskriva åtgärder som kan användas men också belysa de krav som ställs på verksamheten då åtgärden nyttjas. Kraven som här åsyftas är bland annat arbetsrättsliga lagar och regelverk, likväl som lagar och regler kopplade till intrång i den personliga integriteten.

Att tänka på!

- Åtgärderna bör inte begränsas till anställda - även konsulter och leverantörer som deltar i verksamheten kan vara föremål för åtgärder.
- Det är viktigt att säkerställa att relevanta åtgärder inom medarbetarsäkerhet vidtas då en medarbetare byter tjänst inom verksamheten.

4.1 Före anställning

Redan inför anställning av nya medarbetare bör arbetet med medarbetarsäkerhet påbörjas. En väl genomförd rekryteringsprocess är ett väsentligt verktyg för att skapa en bild av lämpligheten av en person som kan komma att anställas i verksamheten. En organisations åtgärder för att hantera risken för möjliggörare börjar därför i rekryteringsprocessen.[28]

Inför en rekryteringsprocess bör en bedömning av den aktuella rollen göras mot den riskanalys som gjorts. Bedömningen bidrar till att avgöra omfattning på de åtgärder som ska utföras inom ramen för medarbetarsäkerhet. Bedömning av en tjänst redan innan rekryteringen påbörjas möjliggör att vid utannonsering tydliggöra att tjänsten kräver att kandidaten är lämplig ur ett säkerhetsperspektiv. Det kan även förtydligas att exempelvis bakgrundkontroll erfordras för tjänsten eller att drogtester kan förekomma. Här kan det vara passande att rekryterande chef samarbetar med HR-funktionen och säkerhetsfunktionen för att säkerställa lämpliga formuleringar.[29] Formuleringarna bör göras på strategisk nivå och återanvändas för att säkerställa en sammanhållen kommunikation i frågorna. Att göra en bedömning av behovet av säkerhetsåtgärder kan bidra till att rekryteringensprocessen sker så effektivt som möjligt utifrån verksamhetens behov, detta då åtgärder som exempelvis bakgrundskontroll kan vara tidskrävande.

[28] *National Insider Threat Center, (2018). CERT Common Sense Guide to Mitigating Insider Threats.*

[29] *Brå, (2024). Möjliggörare för kriminella nätverk - Om möjliggörare i kommunal, statlig och privat sektor. Rapport 2024:2.*

När rekryteringsprocessen går mot sitt slut och en slutkandidat finns, är det lämpligt att genomföra eventuell bakgrundskontroll och/eller drogtest innan avtal signeras. Åtgärderna bör endast genomföras på slutkandidaten och avtalet bör signeras först när resultatet av bakgrundskontroll och drogtest kommit tillbaka, och endast om resultatet anses tillfredsställande.

Bakgrundskontroll, drogtest och avtalssignering är tre åtgärder inom området medarbetarsäkerhet som kan tillämpas före en anställning av en medarbetare, se figur 2. Utöver dessa tre åtgärder bör även interna riktlinjer och policyer finnas på plats, då dessa är en förutsättning för säkerhetsarbetet.

Figur 2 - Åtgärder att tillämpa inom ramen för medarbetarsäkerhet före anställning av en ny medarbetare.

4.1.1 Interna riktlinjer, policyer och dokument

Tydliga och relevanta policyer och riktlinjer tillsammans med andra interna dokument som berör medarbetarsäkerhet bör finnas på plats innan medarbetare börjar. Genom att ha tydliga policyer och riktlinjer har medarbetare möjlighet att tidigt tillgå information som vägleder säkerhetsarbetet i verksamheten samt hur medarbetare ska agera i säkerhetsfrågor. Policyer och riktlinjer bör hållas koncisa och behöver vara sammanhängande för att skapa en tydlighet.

Innehållet i riktlinjer och policyer kopplat till medarbetarsäkerhet bör utgå från en genomförd analys av verksamheten och dess risker. Att en sådan analys gjorts kan säkerställa att medarbetare känner sig sedda och trygga i hur regleringen av deras arbetsplats och vardagliga arbete sker.[30] Policyer och riktlinjer kan exempelvis innehålla information om uppförande inom verksamhetens värderingar, rapporteringsvägar eller information om medarbetarens ansvar inom säkerhetsarbetet. De bör även, om tillämpligt, innehålla information om varför de appliceras inom verksamheten. Syftet med detta är att skapa förståelse hos medarbetare om varför vissa åtgärder behövs eller skulle kunna komma behövas.

[30] *National Insider Threat Center, (2018). CERT Common Sense Guide to Mitigating Insider Threats.*

Det är viktigt att implementering och tillämpning av interna policyer och riktlinjer sker enhetligt och konsekvent för att undvika att medarbetare känner sig särbehandlade eller går miste om nödvändig information.[31] Interna riktlinjer och policyer kan bland annat användas för att informera medarbetare om deras skyldigheter. Detta exempelvis rörande rapportering av incidenter gällande möjliggörare eller hur information som medarbetaren tillgodogjort sig i arbetet får användas, där det senare kan även regleras i anställningsavtal.

4.1.2 Bakgrundskontroll

Syftet med en bakgrundskontroll är att säkerhetsställa riktigheten i informationen den arbetssökande uppger om sig själv, men också att kunna upptäcka eventuella oegentligheter i personens förflutna eller sårbarhet för externa påtryckningar. Huruvida en bakgrundskontroll ska genomföras, samt omfattningen av kontrollen, bör grunda sig i genomförd riskanalys. För de fall en verksamhet ser behov av att genomföra bakgrundkontroller är det viktigt att juridiska krav beaktas. Verksamheten bör ta fram en policy för bakgrundskontroller som behandlar den rättsliga grund som finns för att genomföra bakgrundskontroll. Policyn bör även behandla hur anställningsbeslut fattas utifrån den information som kontrollen visar, samt vilka personer inom verksamheten som får ta del av information som framkommit under kontrollen. En sådan policy bör också specificera hur information från kontrollen ska lagras och hur och när informationen ska raderas.[32] Då bakgrundskontroller är integritetskänsligt kan det vara lämpligt att involvera den lokala fackföreningen i en dialog om att bakgrundskontroller genomförs, eller kan komma att genomföras.

På grund av den integritetskänsliga aspekten av bakgrundskontroller, samt att det i samband med bakgrundkontroll samlas in en stor mängd personuppgifter om enskilda individer, behöver hänsyn tas till den personliga integriteten i arbetet med dessa kontroller. Eftersom en bakgrundskontroll kan anses kartlägga enskildas personliga förhållanden måste samtycke inhämtas från den person en bakgrundskontroll ska utföras på. Den personliga integriteten skyddas i regeringsreformen; i 2 kap. 6 § står att: ”…var och en [är] gentemot det allmänna skyddad mot betydande intrång i den personliga integriteten, om det sker utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden”.[33]

Enligt dataskyddsförordningen (GDPR) är samtycke en av de grunder som finns för laglig behandling av personuppgifter.[34] Samtycke anses dock inte vara ett fullgott skäl som rättslig grund för en arbetsgivare vid behandling av personuppgifter vid en bakgrundskontroll, då arbetstagaren kan anses stå i beroendeställning till arbetsgivaren.[35,36] Verksamheten måste således ha ytterligare rättslig grund att luta sig mot vid insamling av personuppgifter. Insamlingen av personuppgifter måste dessutom vara för ett uttryckligt angivet ändamål, uppgifterna måste ha relevans för ändamålet, inte vara för omfattande och de får inte heller användas på annat sätt än vad som är förenligt med ändamålet.[37] Detta medför att den kontroll

---

[31] *National Insider Threat Center, (2018). CERT Common Sense Guide to Mitigating Insider Threats.*

[32] *National Insider Threat Center, (2018). CERT Common Sense Guide to Mitigating Insider Threats.*

[33] *SFS 2010:1408 Lag om ändring i regeringsformen.*

[34] *EU:s dataskyddsförordning 2016/679 (GDPR).*

[35] *Integritetsmyndigheten, Rättslig grund. Hämtad: 2024-03-14.*

[36] *SOU 2019:19 Belastningsregisterkontroll i arbetslivet – behovet av utökat författningsstöd.*

[37] *EU:s dataskyddsförordning 2016/679 (GDPR).*

som görs och information som samlas in måste stå i proportion till den roll som personen utreds för.

Det är vanligt att genomförandet av bakgrundskontroll åläggs en tredje part. Att nyttja ett professionellt externt företag för att genomföra bakgrundskontroller är ett sätt att säkerställa att bakgrundskontrollen genomförs enligt befintliga regelverk samt att uppgifterna som samlas in hanteras korrekt.

Sammanfattningsvis måste det finnas ett berättigat intresse för bakgrundskontrollens genomförande och kontrollen måste dessutom stå i proportion till syftet. Personen som ska kontrolleras måste ge samtycke till kontrollen, samt informeras om vilka personuppgifter som kommer samlas in och hur dessa kommer att behandlas. Utöver detta måste personen ha möjlighet att ta tillbaka sitt samtycke.

4.1.2.1 Vad kan kontrolleras?

En bakgrundskontroll kan innefatta olika aspekter och det finns ingen definition av vilka delmoment som en bakgrundskontroll ska innehålla. Exempel på delmoment inom en bakgrundskontroll är: CV-kontroll, kreditupplysning, bolagsengagemang, kontroll av belastningsregister, sanktionslistor och civilrättsliga tvister samt genomgång av exponering i media och social media. I vissa fall görs även bakgrundskontroll av make/maka/sambo/partner. Omfattningen av en bakgrundskontroll, det vill säga vad den innefattar och hur långt tillbaka i tiden kontrollen görs, måste anpassas i enlighet med riskanalysen för befattningen. Eftersom en bakgrundskontroll kan innefatta olika kontroller är det viktigt att den person som ska kontrolleras informeras om vad som ska undersökas. Utöver detta är det viktigt att också kommunicera hur informationen lagras och vilka som kommer kunna ta del av informationen.

CV-kontroll

En vanlig kontroll inför rekrytering är att ta referenser för att väga in andras syn på den person som eventuellt ska rekryteras. En CV-kontroll går steget längre då den avser att säkerställa att det CV personen lämnat är fullständigt och riktigt. CV-kontrollen omfattar kontroller med tidigare arbetsgivare huruvida personen varit anställd på arbetsplatsen samt kontroller gentemot akademiska institut om huruvida personen har genomfört utbildning hos dem. Vid uppringning av en referensperson är det rekommenderat att ringa via företagets växel i stället för den arbetssökandes angivna telefonnummer. Detta säkerställer att den som kontaktas faktiskt arbetar på det angivna bolaget.

Det är inte självklart att en arbetsgivare eller en akademisk institution lämnar ut uppgifter om huruvida en person har arbetat/studerat hos dem, med hänvisning till GDPR. Detta kan vara extra komplicerat om erfarenheten som ska styrkas kommer från annat land. I ett sådant fall kan exempelvis arbetsgivarintyg, betyg, lönespecifikationer eller dylikt begäras in. Vilket underlag som då är tillräckligt för att styrka erfarenheten bör bedömas utifrån helheten av det samlade materialet.

Kreditupplysning

Bakgrundskontroller omfattar i vissa fall kreditupplysning. Kreditupplysning av en fysisk person får enligt kreditupplysningslagen (1973:1173) endast ske om det finns en legitim anledning att genomföra kontrollen. En sådan anledning skulle kunna vara anställning i en roll med ekonomiskt ansvar där en ekonomisk riskbedömning av personen är relevant. Även vid

inhämtning av kreditupplysning är det viktigt att säkerställa att hantering av informationen sker i enlighet med GDPR.

Media och social media

För rekrytering till vissa typer av roller kan det vara relevant att se över kandidatens exponering i media och i social media. Kontroll av en arbetssökandes sociala medier utgör en gråzon för vad som kan anses vara lämpligt och inte, detta då kontroll av sociala media kan anses vara kontroll av information av helt privat karaktär och därmed inte ha någon relevans för yrkesrollen.[38] En kontroll av sociala media kan medföra att man som företag riskerar att hantera personuppgifter som inte är relevanta för ändamålet, något som inte är tillåtet enligt GDPR. Vanligt tycks vara att kontroll av media och social media framför allt sker vid tillsättning av högre tjänster.

Bolagsengagemang

Inom ramen för en bakgrundskontroll är det också vanligt att undersöka den ansökandes aktuella och tidigare bolagsengagemang. Detta för att säkerställa att personen inte bedrivit eller ansvarat för verksamhet som varit föremål för brott eller annan form av tveksamt affärsutövande. Kontrollen avser även att undersöka om den arbetssökande bedriver konkurrerande verksamhet.

Sanktionslistor

För vissa typer av roller kan det vara relevant att kontrollera huruvida personen eller företag förknippade med personen finns med på sanktionslistor. Sanktionslistor kan bland annat lista personer eller företag som är föremål för finansiella sanktioner på grund av penningtvätt eller terrorfinansiering. Exempel på denna typ av sanktionslistor är OFAC US Sanction Program och EU Commision Sanction list. Att kontrollera relevanta sanktionslistor är ett sätt att undersöka om personen som är föremål för bakgrundskontrollen efterlever internationella lagar och regler. Vilka listor som kontrollen sker mot måste avgöras utifrån aktuell tjänst.

Brottmål och civilrättsliga tvister

Som en del av en bakgrundskontroll är det vanligt att kontrollera om den arbetssökande blivit dömd för brott eller förekommit i tvistemål. Generellt gäller att de flesta handlingar inom domstolars verksamhet är allmänna handlingar, vilket innebär att de kan begäras ut av allmänhet och massmedia med stöd i Offentlighets- och sekretesslagen (2009:400) så länge de inte är sekretessbelagda.[39] Vid utlämning av allmän handling sker alltid en sekretessprövning.

Att domar är offentliga nyttjas bland annat av personsökningstjänster som sammanställer denna typ av information och innehar utgivningsbevis, vilket innebär att de har grundlagsskydd enligt Yttrandefrihetsgrundlagen (1991:1469) för insamling och publicering av personuppgifter i sina egna databaser och därmed kan vara undantagna regler inom GDPR.[40] Sådana personsökningstjänster är exempel på källor som ibland nyttjas inom ramen för en bakgrundskontroll. Denna typ av tjänster är dock problematiska ur perspektivet att vem som

---

[38] *Brå, (2024). Möjliggörare för kriminella nätverk - Om möjliggörare i kommunal, statlig och privat sektor. Rapport 2024:2.*

[39] *Sveriges domstolar, Detta blir offentligt. Hämtad: 2024-04-09.*

[40] *Integritetsmyndigheten, Kan jag kräva att uppgifter om mig på Mrkoll, Eniro, Hitta.se, Lexbase, Ratsit och Merinfo tas bort? Hämtad: 2024-04-09.*

helst kan nyttja dem, något som innebär att de också kan användas av kriminella nätverk för att kartlägga potentiella möjliggörare.

Genomförs kontroll av brottmål och civilrättsliga tvister måste även i detta fall hantering av den information som framkommer hanteras korrekt, detta då det är generellt förbjudet att behandla personuppgifter om lagöverträdelser.[41]

Kontroll av belastningsregister

Inom finansiell sektor är det idag vanligt att som en del av en bakgrundskontroll begära utdrag ur den arbetssökandes belastningsregister. Företag inom finansiell sektor, med undantag för försäkringsdistribution, har dock inte något författningsstöd för att kräva utdrag ur belastningsregistret.[42,43] Detta till trots är det vanligt att företag ber om att få se ett registerutdrag inför anställning. För att arbetsgivaren ska kunna se ett utdrag måste den arbetssökande själv begära ut och visa upp detta. Samma förfarande gäller även för den som ska arbeta med försäkringsdistribution. Förfarandet har då författningsstöd enligt lag (2018:1219) om försäkringsdistribution och utdraget från registret omfattar då endast de delar i belastningsregistret som bedömts vara relevanta för arbete inom just försäkringsdistribution.

Att som privatperson begära ut ett registerutdrag för sig själv är en rättighet. Idag finns inget förbud mot att en arbetsgivare begär att få se ett sådant utdrag. Dock finns en oro om att detta är något som skulle kunna missbrukas av arbetsgivare, vilket i längden skulle kunna innebära begränsningar i hur utdrag ur registret kan göras.[44] En sådan begränsning skulle innebära försvårande omständigheter vid bakgrundkontroller inom den finansiella sektorn.

I Statens offentliga utredning *Registerutdrag i arbetslivet* (SOU 2014: 48)[45] analyserades finansiella företags behov av att kontrollera registerutdrag i samband med nyanställning. Även om utredningen konstaterade att finansiell sektor utgör en samhällsviktig funktion bedömde utredningen att författningsreglerad kontroll av registerutdrag inom sektorn inte är skälig. I SOU 2019:19 görs dock bedömningen att finansiella företag bör ha rätt att kontrollera huruvida den som ingår, eller ska ingå, i ledningen förekommer i belastningsregistret. Utöver detta lyfts även ett behov av normgivningsbemyndigande som skulle kunna ge finansiella företag rätt att få begära att en enskild inför anställning visar upp registerutdrag. Detta skulle kunna gälla om det är nödvändigt för att avgöra om den enskilde är lämplig för anställning med hänsyn till befattningens funktion. Bemyndigandet gäller endast befattningar där en lämplighetsprövning anses nödvändig och medger inte löpande kontroll av registerutdrag under anställningen; avgränsningar som görs med hänsyn till skyddet för den personliga integriteten.[46] Utöver detta

---

[41] *Integritetsmyndigheten, Brottsuppgifter. Hämtad: 2024-03-14.*

[42] *SFS 1998:620 Lagen om belastningsregister.*

[43] *Kontroll av belastningsregister som genomförs med stöd av lagen (2018:1219) om försäkringsdistribution har enligt SOU 2014:48 tillkommit på grund av EU-direktiv, inte ur nationella förutsättningar eller riskbedömningar.*

[44] *PROP 1997/1998:97 Polisens register.*

[45] *SOU 2014:48 Registerutdrag i arbetslivet.*

[46] *SOU 2019:19 Belastningsregisterkontroll i arbetslivet – behovet av utökat författningsstöd.*

innehåller CER-direktivet krav på bakgrundskontroller av medarbetare inom så kallade kritiska entiteter.[47,48]

I de fall där utdrag ur belastningsregister uppvisas av den arbetssökande inför nyanställning är det viktigt att känna till hur dokumentation av detta får ske. Utan särskilt författningsstöd är det förbjudet att behandla personuppgifter om lagöverträdelser. Har man som arbetsgivare författningsstöd för att ta del av registerutdraget finns det angivet i aktuell författning om vilka uppgifter som får hanteras och hur. Viktigt att notera är att GDPR kan bli tillämplig även om arbetsgivaren endast behandlar uppgifter på papper; även ett notat om att registerutdrag visats upp är att se som en personuppgift.[49]

Kontroll av närstående

För framför allt höga tjänster kan riskanalysen visa på behov av att även genomföra bakgrundskontroll av närstående såsom make/maka/sambo/partner. Omfattningen av en sådan kontroll bör också baseras riskanalysen. På samma sätt som för den som ska anställas är det mycket viktigt att inhämta samtycke från den som ska kontrolleras samt informera om vad som kommer kontrolleras, hur personuppgifter kommer lagras, vilka som kommer få tillgång till uppgifterna samt hur de raderas.

4.1.2.2 Hur hanteras resultatet av en bakgrundskontroll?

Med utgångspunkt i bakgrundkontrollens resultat görs en bedömning om personen är lämpad för anställning i verksamheten. Beslutet bör tas i enlighet med verksamhetens policy för bakgrundskontroller. Till exempel kan en person med flertalet betalningsanmärkningar eller utmätningar vara extra sårbar för utpressning och en tjänst där stora ekonomiska summor hanteras kan därför anses opassande. Även här är det av yttersta vikt att verksamheten själv avgör vilka typer av uppgifter som kan ha bäring på den kommande anställdas eventuella lämplighet att verka inom verksamheten eller inom en viss befattning i verksamheten. Om det under bakgrundskontrollen framkommer information som kan påverka rekryteringen av den nya medarbetaren kan det vara lämpligt att ha ett uppföljande samtal med den tilltänka medarbetaren. Samtalet kan påvisa om det som avvikit i bakgrundskontrollen kan ha en rimlig förklaring, eller anses som icke relevant för den tjänst som personen ska tillträda.

Det är viktigt att efter bakgrundskontrollen säkerställa att resultatet hanteras på rätt sätt avseende GDPR. Detta innebär att säkerställa att endast de som ska ha tillgång till informationen har det, att informationen sparas på rätt sätt samt att informationen raderas vid rätt tillfälle.

4.1.3 Drogtest

Att genomföra drogtest inför en anställning kan vara en åtgärd inom ramen för medarbetarsäkerhet. Regeringsreformen 2 kap 6 § säger att var och en gentemot det allmänna är

---

[47] *Dir. 2023:30 Genomförande av EU:s direktiv om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen och EU:s direktiv om kritiska entiteters motståndskraft.*

[48] *Dir. 2022/2557 Europaparlamentets och rådets direktiv (EU) 2022/2557 av den 14 december 2022 om kritiska entiteters motståndskraft och om upphävande av rådets direktiv 2008/114/EG.*

[49] *Integritetsmyndigheten, Brottsuppgifter. Hämtad: 2024-03-14.*

skyddad mot påtvingat kroppsligt ingrepp vilket innebär att en offentlig arbetsgivare generellt inte kan tvinga någon att genomföra ett drogtest, undantaget är dock drogtester som genomförs med stöd av 30 § i lagen (1994:260) om offentlig anställning (LOA).[50] Inom privat sektor kan, enligt praxis, rätten att genomföra alkohol- eller drogtester avtalas mellan arbetsgivare och arbetstagare.[51] Inom privat sektor gäller dock att ingen kan tvingas av sin potentiella arbetsgivare att genomföra ett drogtest. Att vägra genomföra ett test kan dock vara skäl att neka anställning.

Som arbetsgivare behövs generellt ett relevant skäl för att drogtester genomförs. Ett sådan skäl kan exempelvis vara säkerhet eller en drogfri arbetsmiljö.[52] Att drogtest genomförs inför en anställning bör stå i jobbannonsen. Utöver detta kan det vara bra att ha en alkohol- och drogpolicy som beskriver arbetsplatsens syn på alkohol och droger, vilka regler som gäller på arbetsplatsen, hur förfarandet med tester ser ut samt hur eventuella positiva testresultat hanteras.

Drogtester inför anställning görs generellt med stöd av samtycke från den arbetssökande. Samtycket är dock påkallat i och med att den som söker tjänsten står i beroendeställning till verksamheten, något som innebär att det kan ifrågasättas ur ett arbetsrättsligt perspektiv. Detta, samt att det kan anses integritetskränkande att genomföra drogtester, innebär att det kan finnas fördelar med att ta fram och förankra en alkohol- och drogpolicy med de fackliga representanterna på arbetsplatsen.

4.1.4 Avtalssignering

När rekryteringsprocessen inklusive eventuell bakgrundskontroll och drogtest är klar ska ett anställningsavtal tecknas. Ett vanligt anställningsavtal kan användas för att reglera hur och vilken information medarbetaren får använda på sin nya arbetsplats. Avtalet kan även precisera medarbetarens ansvar för verksamhetens säkerhet samt medarbetarens skyldighet att på uppmaning lämna drogtest, till exempel genom hänvisning till verksamhetens riktlinjer, regler eller policyer.

Inför en anställning kan även sekretessavtal, eller Non Disclosure Agreement (NDA), tillämpas. Ett sekretessavtal är juridiskt bindande och syftar till att skapa ett åtagande för medarbetaren som signerar avtalet att hemlighålla information som denne får ta del av inom ramen för anställningen. Avtalet kan förtydliga vilken typ av information som kan vara av känslig karaktär och som kan utgöra en sårbarhet för medarbetaren och verksamheten om den används felaktigt eller sprids för allmänheten. Hur verksamheters information ska, och får, hanteras regleras även av bland annat lag (2018:558) om företagshemligheter, offentlighets- och sekretesslagen (2009:400), banksekretess, eller upphovsrätts- och dataskyddslagstiftning. Ett sekretessavtal bör därför utformas i linje med, och som ett komplement till, relevant lagstiftning.

[50] *SFS 1994:260. Lagen om offentlig anställning.*

[51] *SOU 2009:44 Medicinska undersökningar – gällande regler och praxis.*

[52] *Ibid.*

Generella skrivningar i anställningsavtal och sekretessavtal bör tas fram strategiskt. Ett sådant arbete kan med fördel utgå ifrån standarder som exempelvis ISO 27002:2022. Det bör också framgå av avtalen vad som gäller i händelse av att den anställde bryter mot avtalet.

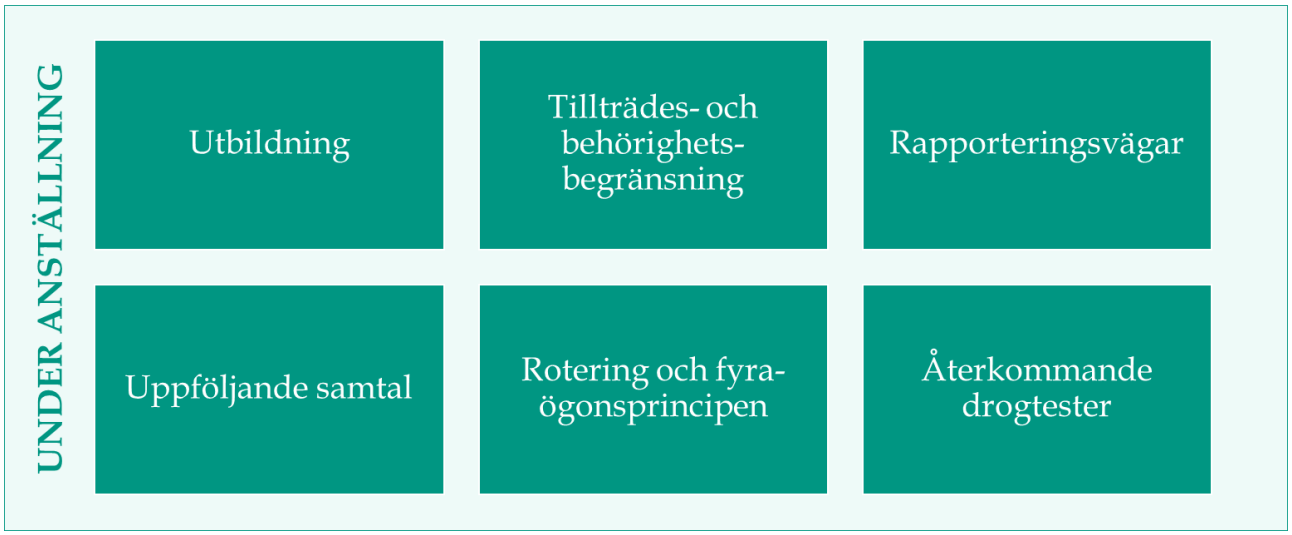
Att tänka på!

- Avtalssignering och sekretessavtal kan vara relevant att se över även för leverantörer som på något sätt ska delta i verksamheten.

4.2 *Under anställning*

När ett avtal signerats och en medarbetare ska börja arbeta i verksamheten är det viktigt att denne tidigt blir insatt i säkerhetsarbetet och erhåller den kunskap och förståelse som behövs för den aktuella tjänsten. Har verksamheten en stark säkerhetskultur kan det även bidra till att öka medarbetarens engagemang för, och vilja till, att bidra till en god säkerhet. I början av en medarbetares anställning kan det vara bra att dokumentera utlämning av material såsom teknisk utrustning och dokumentation som medarbetaren får tillgång till. Detta för att underlätta för den avslutningsprocess som kommer den dag då medarbetaren lämnar verksamheten.

Inom ramen för medarbetarsäkerhet finns ett antal åtgärder som kan nyttjas för att stärka medarbetarens förståelse för säkerhetsarbetet och som möjliggör för medarbetaren att agera på rätt sätt i säkerhetsrelaterade frågor både inom och utom organisationen. Det finns också åtgärder som kan nyttjas för att undersöka om en medarbetares livssituation förändrats och på så sätt ökat personens sårbarhet som följd. I figur 3 presenteras exempel på åtgärder som kan tillämpas under en anställning inom ramen för medarbetarsäkerhet.



Figur 3 - Åtgärder att tillämpa inom ramen för medarbetarsäkerhet under den tid en medarbetare är anställd.

4.2.1 Utbildning

En förutsättning för att medarbetare ska kunna agera korrekt i säkerhetsrelaterade frågor är att samtliga medarbetare har tillgång till information och får kunskap om hur de ska agera. Detta

bör ske genom fortlöpande säkerhetsutbildningar som innefattar hela verksamheten och där medarbetarsäkerhet är en del av utbildningen. Utbildning kan verka stärkande för en säkerhetskultur och även öka medarbetarnas kunskap om sin yrkesrolls värdegrund och mål.[53]

Syftet med säkerhetsutbildning bör vara att skapa förståelse för hot som föreligger mot verksamheten, vilka åtgärder som vidtas mot dessa hot och den roll som medarbetare har i säkerhetsarbetet. En utbildning kan innehålla svar på frågor som exempelvis:

- Varför arbetar verksamheten med säkerhetsfrågor?
- Varför är säkerhet viktigt?
- Vilka hot finns mot verksamheten?
- Vilka hot kan påverka medarbetare i verksamheten?
- Hur arbetar verksamheten med säkerhetsfrågor?
- Var finns policyer, riktlinjer, rutiner och information om säkerhetsarbetet?
- Vilka säkerhetsåtgärder vidtas?
- Hur ska medarbetaren arbeta på ett säkert sätt?
- Vilka säkerhetsåtgärder bör vidtas vid distansarbete?
- Vem i organisationen kan svara på frågor om säkerhetsarbetet?
- Hur ser rapporteringsvägar ut för rapportering av brister eller oegentligheter?
- Vad händer om en medarbetare rapporterar om en brist eller dylikt?

Eftersom anställda kan få tillgång till information och system kort tid efter att anställning påbörjats bör säkerhetsutbildning för medarbetaren genomföras tidigt i anställningen. Vissa arbetsplatser ger inte tillgång till information och system förrän medarbetaren genomgått en grundläggande säkerhetsutbildning, vilket kan vara en viktig delåtgärd inom ramen för medarbetarsäkerhet. En utbildning som genomförs tidigt påvisar också vikten av säkerhetsfrågor i verksamheten.

Utbildningens innehåll bör anpassas efter den befattning som medarbetaren har. Utbildningsbehov för olika befattningar och rutiner för utbildning bör utgå från verksamhetens riskanalys. Mer fördjupade utbildningar kan krävas för befattningar där tillgång till information och/eller system är betydande. Utöver detta kan specifika chefsutbildningar vara relevanta då chefer ofta är viktiga för säkerhetskulturen på en arbetsplats. Till exempel ska medarbetare ofta vända sig till närmaste chef med frågor eller om något är fel.

Inom ramen för en säkerhetsutbildning bör frågor som rör de sårbarheter och styrkor som medarbetare kan utgöra för verksamhetens säkerhet tas upp. Det är viktigt att ge medarbetarna en förståelse för varför åtgärder som exempelvis bakgrundskontroller, tillträdes- och behörighetsbegränsningar eller uppföljande samtal används inom verksamheten. Förståelse är viktigt för att skapa en miljö där medarbetare inte känner sig misstänkliggjorda utan i stället får insikt i, och kan känna sig stärkta av, att åtgärderna bidrar till att skydda dem från otillbörliga kontakter och möjliggör för dem att agera korrekt, och därmed bidra till verksamhetens säkerhet, i sitt vardagliga arbete.

Ett hot som direkt rör området medarbetarsäkerhet som kan tas upp vid utbildningstillfällen där det är relevant är hotet från möjliggörare. Kunskap om möjliggörare är ofta som störst hos dem

[53] *Brå, (2024). Möjliggörare för kriminella nätverk - Om möjliggörare i kommunal, statlig och privat sektor. Rapport 2024:2.*

som arbetar med säkerhetsrelaterade frågor inom en verksamhet men kunskapen behöver spridas på en bredare front inom verksamheten. Två grupper som är särskilt viktiga att höja kunskapen hos är HR-personal och chefer, men även medarbetare behöver få kunskap om risken för möjliggörare.[54] Eftersom möjliggörare kan handla medvetet men också omedvetet behöver medarbetare få verktyg att förstå vilka handlingar hos en själv eller hos en kollega som bör uppmärksammas.

Kunskap om möjliggörare ökar också medarbetares skydd mot att själv stå föremål för att bli en möjliggörare.[55] En utbildning kan till exempel beskriva drivkrafter till varför en medarbetare blir möjliggörare samt även belysa att medarbetare kan bli närmade utanför arbetstid och arbetsplatsens lokaler. Sociala medier som LinkedIn och andra öppna informationsskällor kan användas av externa parter för att söka medarbetare som skulle kunna bli möjliggörare.[56] Det kan också vara relevant att i utbildningen beröra rutiner vid distansarbete samt arbete i offentlig miljö. Genom utbildningar där risken för möjliggörare berörs får medarbetare den kunskap de behöver för att både kunna utföra eget arbete och arbetsuppgifter på ett säkert och tillfredställande sätt, samtidigt som de erhåller verktyg för att kunna uppmärksamma tecken på om någon agerar som möjliggörare.

Det är viktigt att utbildning även tar upp information om rapporteringsvägar vid avvikelser i informationshantering, förlust av information, slarv, eller liknande, för att säkerställa att alla medarbetare vet vem i verksamheten som kan kontaktas vid behov. Medarbetare bör också upplysas om det ansvar som föreligger dem att uppmärksamma brister i verksamheten som skulle kunna utgöra en sårbarhet för både verksamheten i sig och för andra medarbetare. Detta beskrivs ytterligare under avsnitt 4.2.3 Rapporteringsvägar.

Fortlöpande utbildningar ska ses som ett komplement till tydliga interna riktlinjer, policyer och andra dokument med skriftlig information. Det är av särskild vikt att kunskapshöjande insatser eller längre utbildning sker om något förändras i verksamhetens interna rutiner. Det är även viktigt att behov av utbildning ses över i samband med att en medarbetare byter befattning.

Kontinuerlig utbildning i säkerhetsfrågor bidrar också till en stark säkerhetskultur. Medarbetare som har rätt nivå av kunskap har lättare ta ansvar för säkerhetsfrågor och rapportera eventuella brister. Tillräckliga instruktioner och rutiner som finns att tillgå i till exempel skriftligt format är väsentligt för att medarbetare ska ha tillräcklig medel för att hantera olika situationer.[57] Kunskap, engagemang och utbildning lägger grunden för en organisatorisk säkerhetskultur, men därtill krävs tydlig styrning och tydliga rapporteringsvägar - det behöver vara enkelt att göra rätt. Sammantaget bidrar detta till att medarbetare uppmuntras att rapportera säkerhetsrelaterade brister hos verksamheten.

---

[54] *Brå, (2024). Möjliggörare för kriminella nätverk - Om möjliggörare i kommunal, statlig och privat sektor. Rapport 2024:2.*

[55] *Ibid.*

[56] *Svenska Bankföreningen, (2024). Hotbildsbedömning för Sveriges Banker.*

[57] *Brå, (2024). Möjliggörare för kriminella nätverk - Om möjliggörare i kommunal, statlig och privat sektor. Rapport 2024:2.*

4.2.2 Tillträdes- och behörighetsbegränsning

Eftersom en av möjliggörarens vanligaste uppgifter är att lämna ut information, är en viktig del av medarbetarsäkerhet att säkerställa att endast behöriga medarbetare har tillgång till särskilda fysiska lokaler, särskild information och specifika system. Detta är också viktigt för att skydda medarbetarna från att ha tillgång till mer information än vad arbetet kräver samt för att förhindra misstag.

Tillträdesbegräsning som åtgärd inom medarbetarsäkerhet handlar främst om att begränsa vilka lokaler medarbetare inom den egna verksamheten har tillgång till, men det handlar också delvis om att begränsa åtkomst till lokaler för utomstående.[58] För besökare kan tillträdesbegränsning innebära att besökare möter en bemannad reception där de måste anmäla sig, att de endast får röra sig i ”externa” lokaler samt att de måste ha eskort när de rör sig i lokalerna. Vilket tillträde som ges en medarbetare bör baseras på genomförd riskanalys kopplad till befattning, för att säkerställa att endast medarbetare med behov av särskilt tillträde också är de enda som har detta. Vilken typ av tillträde en person har kan vid behov synliggöras på id-brickor för legitimering för att på så sätt tydliggöra var i verksamhetens lokaler en medarbetare får röra sig. Tillträdesbegränsning måste ses över och uppdateras kontinuerligt, för att säkerställa att förändringar i organisationen återspeglas i vem som har tillgång till vad. Att ha tillträdesbegränsningar innebär också att visst typ av arbete eller arbetsuppgifter bör hänvisas till specifika delar av lokalerna.

Behörighetsbegräsningar i verksamhetens IT-system är också en viktig åtgärd inom ramen för medarbetarsäkerhet. Detta är också något som kravställs den finansiella sektorn i bland annat DORA (Digital Operational Resilience Act), där kommande tekniska standard för IKT-riskhantering kommer beskriva närmare hur kraven ska implementeras i verksamheten.[59] Behörighetsbegränsningar ska säkerställa att medarbetare endast har tillgång till information som behövs för att utföra sitt arbete. En medarbetare bör inte ha tillgång till mer information än nödvändigt och bör inte ha möjlighet att utföra arbete i system de inte behöver för sitt yrkesutövande. Behörighetsbegränsningar, liksom tillträdesbegränsningar, bör baseras på resultatet av genomförd riskanalys och medarbetarens befattning och bör ses över med regelbundenhet. Behörigheter måste kunna dras tillbaka och läggas till utifrån behov och det är mycket viktigt att säkerställa att behörigheter ses över då en medarbetare byter tjänst inom verksamheten.

Det kan även vara relevant att se över vilken typ av behörighetsbegränsningar som bör gälla vid distansarbete, detta då åtkomstbegränsningar för viss information utanför verksamhetens lokaler kan vara relevant.[60]

---

[58] *Ibid.*

[59] *European Banking Authority (2024), Final report Draft Regulatory Technical Standards to further harmonise ICT risk management tools, methods, processes and policies as mandated under Articles 15 and 16(3) of Regulation (EU) 2022/2554.*

[60] *Brå, (2024). Möjliggörare för kriminella nätverk - Om möjliggörare i kommunal, statlig och privat sektor. Rapport 2024:2.*

4.2.3 Rapporteringsvägar

För att säkerställa god medarbetarsäkerhet där medarbetare ges möjlighet att ta ansvar för en stark säkerhetskultur, är det viktigt att det finns tydliga rapporteringsvägar. Dessa bör beskrivas i policyer eller riktlinjer. Rapporteringsvägarna ska kunna användas vid påträffad avvikelse, misstänkt beteende eller om en medarbetare behöver stöd i att upprätthålla sin roll i organisationens säkerhetsarbete. En stark säkerhetskultur, i vilken rapportering ses som en självklarhet och det finns fungerande rapporteringsvägar, kan möjliggöra för att tidigt införa åtgärder mot säkerhetsbrister eller en eventuell möjliggörare och på så sätt förhindra skador av allvarlig karaktär.[61]

Rapporteringsvägar kan bestå av en särskild visselblåsarfunktion eller andra vägar för incidentrapportering. Detta kan med fördel vägas samman med redan existerande rapporteringsvägar inom verksamheten. Oavsett hur rapporteringsvägarna ser ut behöver de vara lättförståeliga, åtkomliga och tillgängliga för samtliga medarbetare inom verksamheten. Eftersom det kan uppfattas som känsligt att exempelvis rapportera en kollega är det av yttersta vikt att samtliga medarbetare känner sig trygga med de interna rapporteringsvägarna och att de har kännedom om hur informationen de lämnar ifrån sig kan komma att behandlas.

För att medarbetare ska känna sig trygga i vad som kan lyftas via officiella rapporteringsvägar bör detta vara ett delmoment i fortlöpande utbildningar. Medarbetare bör uppmärksammas på vilka typer av signaler eller handlingar som kan utgöra grund för rapportering, som till exempel kännedom om mutor, hot eller annan form av utpressning, jäv eller för verksamheten olämpliga relationer.[62]

4.2.4 Uppföljande samtal

För att möjliggöra uppföljning av en bakgrundskontroll under anställningens gång, eller för att initiera samtal med medarbetare som anställdes innan en rutin för bakgrundskontroll kommit på plats, kan uppföljande samtal genomföras. Syftet med ett sådant samtal är främst att skapa ett forum där förändringar hos medarbetaren kan fångas upp, om medarbetaren har påverkats av någon händelse, hamnat i trångmål eller liknande.[63]

Det uppföljande samtalet kan med fördel genomföras av närmaste chef med personkännedom om medarbetaren och kan sammanfalla med årliga medarbetarsamtal eller liknande. För chefer finns det anledning att vara uppmärksam på medarbetarnas mående generellt, för att i god tid kunna uppmärksamma om något hos medarbetaren skulle förändras och därmed göra den mer sårbar för att bli en möjliggörare.[64] En god arbetsmiljö där medarbetare har förtroende för sina närmsta chefer skapar också möjligheter för att medarbetarna själva ska ta initiativ till sådana samtal, ifall behov skulle uppstå.

Likt problematiken med bakgrundskontroller finns frågan om var gränsen för den personliga integriteten går vid ett uppföljande samtal där en individs sårbarheter sätts i fokus. Dessa samtal

---

[61] *Ibid.*

[62] *Ibid.*

[63] *Brå, (2024). Möjliggörare för kriminella nätverk - Om möjliggörare i kommunal, statlig och privat sektor. Rapport 2024:2.*

[64] *Ibid.*

bör därför följa uppsatta interna rutiner som med fördel tagits fram i dialog mellan HR-avdelning samt ansvariga säkerhetsfunktioner. Här bör även arbetsgivares ansvar att förebygga missbruk av till exempel alkohol, narkotika, eller spel, nämnas, då dessa missbruk ofta relateras till sårbarheter som kan få en medarbetare att agera möjliggörare.[65]

Att främja en arbets- och säkerhetskultur där medarbetare känner sig trygga att rapportera om incidenter och sårbarheter utan att riskera att straffas är en åtgärd för att minska stigmat kring medarbetarsamtal av denna karaktär. Det bidrar även till en kultur där medarbetare kan fråga varandra, eller chefer, om råd för att se till att rutiner och riktlinjer efterföljs.

4.2.5 Rotering och fyraögonsprincipen

Ett sätt att försvåra för möjliggörare eller att minimera misstag från medarbetare, är att tillämpa arbetssätt där flera personer involveras innan ett beslut fattas eller en transaktion går igenom. Denna typ av arbetssätt tillämpas ofta inom den finansiella sektorn. I FFFS 2018:16 finns följande råd för en sund riskkultur gällande kreditrisker: ”att ingen person ensam ska handlägga ett kreditärende genom hela kreditgivningsprocessen”.[66] Ibland kallas arbetssättet fyra-ögonsprincipen och kan användas som en åtgärd för att minska korruption och försvåra för möjliggörare. Fyraögonsprincipen kan användas inom flera områden inom den finansiella sektorn. Behovet av att införa fyraögonsprincipen i vissa arbetsflöden bör identifieras i riskanalysen av verksamheten.

Utöver fyraögonsprincipen kan även rotering användas som ett skydd mot att medarbetare upparbetas till möjliggörare. Genom att rotera medarbetare mellan olika roller inom verksamheten byts ansvariga med jämna mellanrum ut. Det gör att samma personer inte alltid har samma behörigheter eller tillgång till information, vilket försvårar en roll som möjliggörare.

4.2.6 Återkommande drogtester

Återkommande drogtester under anställningstiden kan användas för att bland annat identifiera missbruk, något som identifierats som en sårbarhet för att bli möjliggörare.[67] Enligt praxis kan drogtester inom den privata sektorn genomföras om arbetsgivaren avtalat med den anställde om att drogtester kan komma att genomföras under anställningstiden.[68] En medarbetare kan inte tvingas till att genomföra ett drogtest, men att neka till att genomföra ett drogtest kan utgöra skäl för uppsägning om så avtalats. Inom offentlig sektor kan drogtester genomföras med stöd av 30 § i lagen (1994:260) om offentlig anställning (LOA).

4.2.7 Återkommande bakgrundskontroller

Mycket kan förändras i en medarbetares livssituation, speciellt om medarbetaren deltagit i verksamheten under lång tid, och förändringar kan påverka en persons sårbarhet. För att fånga in denna typ av förändringar lyfts ofta frågan om återkommande bakgrundskontroller kan

---

[65] *Ibid.*

[66] *FFFS 2018:16 Finansinspektionens föreskrifter och allmänna råd om hantering av kreditrisker i kreditinstitut och värdepappersbolag.*

[67] *Brå, (2024). Möjliggörare för kriminella nätverk - Om möjliggörare i kommunal, statlig och privat sektor. Rapport 2024:2.*

[68] *SOU 2009:44 Medicinska undersökningar – gällande regler och praxis.*

genomföras. Idag genomförs återkommande bakgrundskontroller av befintliga medarbetare med lagstöd inom ramen för säkerhetskänslig verksamhet, men inom icke säkerhetskänslig verksamhet finns inget lagstöd för detta.

Bakgrundskontroller av befintliga anställda och återkommande bakgrundskontroller har varit föremål för diskussion vid flera tillfällen, bland annat när lämplighetsprövning av personal inom skolväsendet infördes. Då valde lagstiftaren att inte låta lagen omfatta redan anställda med hänsyn till den personliga integriteten.[69] År 2023 riktande Justitieombudsmannen (JO) allvarlig kritik mot Södertälje kommun efter införande av löpande bakgrundskontroller av anställda med motiveringen att kontrollerna innebär ett betydande ingrepp i den personliga integriteten samt övervakning och kartläggning av enskildas personliga förhållanden.[70] I beslutet pekar JO även på avsaknaden av lagstöd för att genomföra denna typ av kontroller.

Frågan om det är lämpligt att genomföra återkommande bakgrundskontroller handlar dels om avsaknaden av lagstöd, dels om huruvida en verksamhet kan genomföra detta utan att kränka den personliga integriteten. Vad som gäller är inte självklart, tydligt är dock att en utgångpunkt flera aktörer har är att återkommande bakgrundskontroller inte är lämpligt att utföra, detta bland annat utifrån samtal med referensgrupp för detta PM. Diskussioner pågår dock inom den finansiella sektorn med bland annat arbetsgivarorganisationer för att utreda om, och i så fall i när, återkommande barkgrundskontroller kan vara lämpliga. I Svenska Bankföreningens Hotbildsbedömning för 2024 påtalas exempelvis behovet av tillräckliga kontrollmöjligheter både vid och under anställning.[71]

4.3 Vid avslut av anställning

En tydlig avslutningsprocess för medarbetare som lämnar sin tjänst hos verksamheten bidrar till att verksamhetens arbete med medarbetarsäkerhet är aktiv genom hela anställningen. En sådan process kan innehålla steg som avslutningssamtal och återlämning av material och information. Processen bör utgå från redan tidigare upparbetade rutiner kring avslut av anställning. När en medarbetare lämnar sin tjänst är det viktigt att inte bara följa upp avslutet med personen som lämnar, utan också att meddela samtliga inom verksamheten att medarbetaren har slutat. Detta förebygger att någon inom verksamheten oavsiktligt delar information med eller släpper in den före detta medarbetaren i verksamhetens lokaler.[72]

---

[69] *Prop. 1999/2000:123 Lämplighetsprövning av personal inom förskoleverksamhet, skola och skolbarnsomsorg*

[70] *Justitieombudsmannen (2023). Beslut 2023-10-19 dnr: 7143-2022, Allvarlig kritik mot Kommunstyrelsen i Södertälje kommun för att i strid mot skyddet för den personliga integriteten och privatlivet ha kontrollerat om kommunanställda gjort sig skyldiga till brott*

[71] *Svenska Bankföreningen, (2024). Hotbildsbedömning för Sveriges Banker.*

[72] *National Insider Threat Center, (2018). CERT Common Sense Guide to Mitigating Insider Threats.*

Figur 4 - Åtgärder att tillämpa inom ramen för medarbetarsäkerhet efter avslutad anställning av en medarbetare.

4.3.1 Återlämning av material och utrustning

Medarbetare vars anställning avslutas bör återlämna material så som dator, telefon och annan utrustning som hör till verksamheten. Även dokumentation och information tillhörande verksamheten ska återlämnas eller förstöras. Det är viktigt att medarbetaren uppmärksammas på att det inte är tillåtet att behålla utrustning och/eller information som tillhör verksamheten – särskilt om materialet skulle vara av känslig natur. Det är viktigt att påminna om detta då det finns exempel på situationer där medarbetare vid slutet av en anställning har tagit med sig material och information tillhörande verksamheten till en ny arbetsgivare, utan att förstå varför detta kan åsamka skada och varför de inte var tillåtna att göra en sådan sak.[73] För att påminna om sekretess kan hänvisas till NDA eller anställningsavtal som undertecknats, eller till riktlinjer och policyer medarbetaren godkänt.

Medarbetarens samtliga konton kopplade till tjänsten bör också stängas ned, liksom kreditkort, accesskort och liknande som hör till verksamheten. All sådan utrustning skulle, om den inte återlämnas, i olika omfattning kunna användas för att utöva påtryckning eller försök att komma åt verksamheten efter det att en medarbetares anställning har upphört.

Utarbetade rutiner för inventering av material och utrustning, samt tillträdes- och behörighetsrättigheter underlättar vid avslut av en anställning, då det går att kontrollera att samtligt material är återlämnat. Detta kan med fördel kopplas ihop med en eventuell process som påbörjats vid nyanställning där utlämning av material och utrustning har dokumenterats.[74]

4.3.2 Avslutningssamtal

Ett avslutningssamtal med medarbetaren kan genomföras av dennes närmsta chef eller HR för att delge feedback till medarbetaren, påminna om sekretessavtal eller sekretessklausuler i anställningsavtal, samt fånga upp eventuella frågor och funderingar från medarbetaren. En väl genomförd avslutningsprocess för den medarbetare som lämnar verksamheten bidrar till att

[73] *Brå, (2024). Möjliggörare för kriminella nätverk - Om möjliggörare i kommunal, statlig och privat sektor. Rapport 2024:2.*

[74] *National Insider Threat Center, (2018). CERT Common Sense Guide to Mitigating Insider Threats.*

medarbetaren lämnar verksamheten i god anda, där inga oklarheter eller agg gentemot verksamheten lämnas oberörda. Det skyddar verksamheten mot att individen som lämnar sin tjänst vid ett senare tillfälle har incitament att till exempel sprida känslig information gällande verksamheten.[75]

5 Särskilda krav på säkerhetskänslig verksamhet

Detta kapitel avser att översiktligt beskriva skyddsåtgärder för verksamheter som omfattas av säkerhetsskyddslagen (2018:585), samt att redogöra för generella distinktioner mellan de verksamheter som omfattas och de som inte omfattas av säkerhetsskyddslagen. Denna promemoria redogör inte i detalj hur enskilda verksamheter ska arbeta med säkerhetsskydd, för exakta skrivelser om lagens tillämpningsområde och bestämmelser om säkerhetsskydd hänvisas till:

- Säkerhetsskyddslag (2018:585)
- Säkerhetsskyddsförordningen (2021:955)
- Säkerhetspolisens föreskrifter om säkerhetsskydd (PMFS 2022:1)

Säkerhetspolisen har även gett ut flera vägledningar om säkerhetsskydd, som kan användas av verksamhetsutövare som ett stöd i tillämpningen av regelverket för säkerhetsskydd.

Säkerhetsskyddslagen gäller för verksamheter som helt eller delvis ”[…] är av betydelse för Sveriges säkerhet eller som omfattas av ett för Sverige förpliktande internationellt åtagande om säkerhetsskydd (säkerhetskänslig verksamhet)”.[76] I säkerhetsskyddslagen är säkerhetsskydd beskrivet enligt följande: ”Med säkerhetsskydd avses skydd av säkerhetskänslig verksamhet mot spionerі, sabotage, terroristbrott och andra brott som kan hota verksamheten samt skydd i andra fall av säkerhetsskyddsklassificerade uppgifter”.[77]

Säkerhetsskyddslagen omfattar skyddsåtgärder inom följande tre områden:

- Informationssäkerhet
- Fysisk säkerhet
- Personalsäkerhet

Då denna promemoria har huvudsakligt fokus på säkerhetsåtgärder som berör en verksamhets medarbetare kommer fortsatt endast området *personalsäkerhet* beaktas. För åtgärder och förslag på åtgärder att tillämpa inom områdena för informationssäkerhet och fysisk säkerhet hänvisas till bland annat Säkerhetspolisens vägledningar: *Vägledning i säkerhetsskydd Fysisk säkerhet* (2023) och *Vägledning i säkerhetsskydd Informationssäkerhet* (2023).

En förutsättning inom arbetet med säkerhetsskydd, och därmed också personalsäkerhet, är att en säkerhetsskyddsanalys genomförts. Säkerhetsskyddsanalysen ska ”[…] identifiera vilka säkerhetsskyddsklassificerade uppgifter och vilken säkerhetskänslig verksamhet i övrigt som finns i verksamheten samt vilka hot och sårbarheter som finns kopplade till dessa

[75] *Ibid.*

[76] *SFS 2018:585 Säkerhetsskyddslag.*

[77] *Ibid.*

skyddsvärden".[78] Den ska också ligga till grund för bedömningar av vilka befattningar som ska placeras i säkerhetsklass och/eller säkerhetsprövas. Säkerhetsskyddsanalysen kan med fördel ha en förteckning över befattningar med krav på säkerhetsprövning bifogad, där skälet till placering i säkerhetsklass samt beslut om placering av befattning i säkerhetsklass tydligt framgår.[79] Säkerhetsskyddsanalysen ska även omfatta en bedömning av nödvändiga säkerhetsskydds-åtgärder.[80] Behovet av åtgärder kan se olika ut för olika verksamheter, även om de alla omfattas av säkerhetsskyddslagen. Säkerhetsskyddsanalysen ska således ge verksamhetsutövaren en utgångspunkt för att planera för och vidta åtgärder för att hantera säkerhetsskyddsklassificerade uppgifter och säkerhetskänslig verksamhet i övrigt utifrån verksamhetens art och omfattning.

Personalsäkerhet består av områdena *säkerhetsprövning* och *utbildning i säkerhetsskydd*.[81] Åtgärder inom dessa områden ska tillämpas före, under och efter en anställning eller deltagande i säkerhetskänslig verksamhet. De ska, precis som åtgärder inom medarbetarsäkerhet, finnas på plats genom en medarbetares hela deltagande i verksamheten.[82] I likhet med arbetet kring medarbetarsäkerhet fokuserar åtgärder inom ramen för säkerhetsskyddslagen på att säkerställa att verksamheten skyddas från medarbetare som olovligen använder och lämnar ut information till obehöriga, eller på annat sätt skadar verksamheten. Inom säkerhetskänslig verksamhet avser detta säkerhetsskyddsklassificerade uppgifter och säkerhetskänslig verksamhet i övrigt.[83] Det är specifika befattningar inom en verksamhet, eller deltagande i vissa delar av verksamheten, som står i fokus för personalsäkerhet. Viktigt att komma ihåg är att åtgärder inom personalsäkerhet också ska genomföras för leverantörers personal som deltar i verksamheten.

Arbete med säkerhetsskydd är en del av det övergripande säkerhetsarbetet i vilket även medarbetarsäkerhet ingår. Säkerhetsskydd verkar som ett extra lager av åtgärder som appliceras på de verksamheter som faller under säkerhetsskyddslagen. Inom området medarbetarsäkerhet innebär detta att skyddet förstärks genom personalsäkerhetåtgärder, se figur fem. För de som arbetar inom säkerhetskänslig verksamhet ska åtgärder inom personalsäkerhet genomföras enligt lag. En verksamhets åtgärder inom medarbetarsäkerhet fungerar då som ett komplement till personalsäkerhetsåtgärderna.

[78] *SFS 2021:955 Säkerhetsskyddsförordning.*

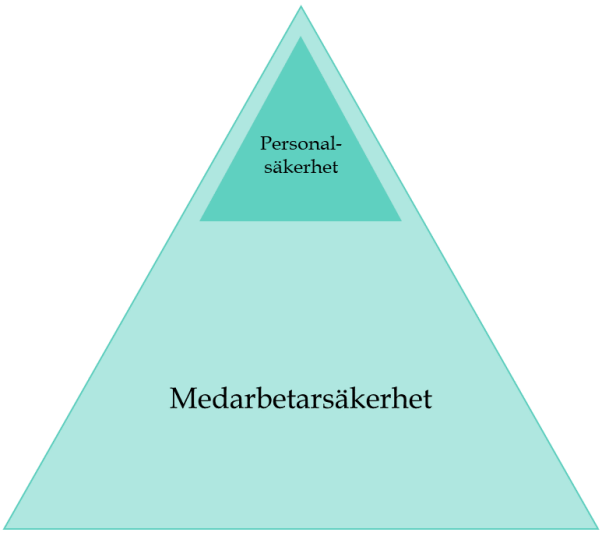
[79] *Säkerhetspolisen, (2023). Vägledning i säkerhetsskydd Personalsäkerhet.*

[80] *Ibid.*

[81] *Ibid.*

[82] *SFS 2018:585 Säkerhetsskyddslag.*

[83] *Ibid.*



Figur 5. Åtgärder inom personalsäkerhetpersonalsäkerhet kan ses som ett extra lager av skydd som appliceras för de medarbetare som ska delta i säkerhetskänslig verksamhet.

5.1 Före deltagande i säkerhetskänslig verksamhet

En rekryteringsprocess till en tjänst inom säkerhetskänslig verksamhet kan vara tidskrävande. Behov kan därför finnas att planera processen internt inom verksamheten innan den påbörjas för att säkerställa att det finns resurser att genomföra den. Det är lämpligt att redan i rekryteringen till en tjänst inom säkerhetskänslig verksamhet informera sökande om att tjänsten kan innebära säkerhetsprövning och registerkontroll.

Att tänka på!

- Även personal från leverantörer som deltar i säkerhetskänslig verksamhet är föremål för åtgärder enligt säkerhetsskyddslagen (2018:585).
- ”En verksamhetsutövare som avser att genomföra en upphandling, ingå ett avtal eller inleda en samverkan eller samarbete med en annan aktör (motpart) ska i de fall som framgår av 4 kap. 1 § säkerhetsskyddslagen (2018:585) ingå ett säkerhetsskydds-avtal”.
- Säkerhetsskyddsavtal syftar till att säkerställa säkerhetsskyddet samt utgöra underlag för beslut om vilka anställningar och deltagande i verksamhet som ska placeras i säkerhetsklass. För vidare information, se Säkerhetspolisens riktlinjer och vägledningar.

5.1.1 Säkerhetsprövning

Säkerhetsprövning ska genomföras för den som genom en anställning, eller på något annat sätt, ska delta i säkerhetskänslig verksamhet.[84] Säkerhetsprövningen ska genomföras *innan* deltagande i säkerhetskänslig verksamhet och gäller för de medarbetare som enligt befattningsanalysen har tillgång till säkerhetsskyddsklassificerade uppgifter, eller kan orsaka skada i verksamhet av betydelse för Sveriges säkerhet. Säkerhetsprövningens syfte är att utreda huruvida medarbetaren anses vara lojal mot de värderingar och intressen som ska skyddas i verksamheten i enlighet med säkerhetsskyddslagen. Prövningen innebär även att klargöra om medarbetaren kan anses vara pålitlig ur ett säkerhetsperspektiv och utreda eventuella sårbarheter.

Inför deltagande i säkerhetskänslig verksamhet består säkerhetsprövningen av en grundutredning inom vilken granskning av betyg och intyg samt andra uppgifter av relevans för prövningen ingår. Utöver detta ingår referenstagning och säkerhetsprövningsintervju i säkerhetsprövningen. Ett samtycke krävs från den person som står föremål för grundutredningen.

När säkerhetsskyddsanalysen påvisar att det finns befattningar inom en verksamhet som ska säkerhetsprövas ska det även utredas huruvida befattningarna ska placeras i säkerhetsklass eller inte. För befattningar som placerats i säkerhetsklass kompletteras säkerhetsprövningen med en registerkontroll. För befattningar placerade i säkerhetsklass 1 och 2 genomförs även en särskild personutredning. Registerkontroll och särskild personutredning genomförs först då medarbetaren har genomgått grundutredning och blivit godkänd i denna. Vid en registerkontroll hämtas bland annat uppgifter från register som omfattas av lagen (1998:620) om belastningsregister eller lagen (1998:621) om misstankeregister. Registerkontroll genomförs av Säkerhetspolisen och innebär en löpande kontroll av individen. För vidare information se Säkerhetspolisens *Vägledning i personalsäkerhet* (2023).

5.1.2 Utbildning

Säkerhetsskyddslagen specificerar att den som bedriver säkerhetskänslig verksamhet har en skyldighet att säkerställa att medarbetare får adekvat utbildning innan deltagande i den säkerhetskänsliga verksamheten. Utbildningen syftar till att medarbetare ska få kunskap om hot och sårbarheter som verksamheten kan utsättas för, om det finns aktuella säkerhetsskyddsåtgärder på plats samt hur det i sådana fall upprätthålls. En del av utbildningen ska även täcka verksamhetens interna bestämmelser. Utbildningen kan också ta upp den tystnadsplikt som gäller samtliga medarbetare som i sin befattning tar del av säkerhetsskyddsklassificerade uppgifter.[85]

5.2 Under deltagande i säkerhetskänslig verksamhet

Under den tid en medarbetare deltar i säkerhetskänslig verksamhet krävs uppföljande säkerhetsprövning och utbildning i säkerhetsskydd.[86]

---

[84] *SFS 2018:585 Säkerhetsskyddslag.*

[85] *Säkerhetspolisen, (2023). Vägledning i säkerhetsskydd Personalsäkerhet.*

[86] *SFS 2018:585 Säkerhetsskyddslag.*

Den uppföljande säkerhetsprövningen genomförs för en bibehållen och fördjupad personkännedom, likt det uppföljande samtal som föreslås som en åtgärd inom området för medarbetarsäkerhet. Syftet med den uppföljande säkerhetsprövningen är att fånga förändringar i en medarbetares lojalitet eller beteende för att på så vis minska risken för skadligt beteende. Precis som för det övergripande säkerhetsarbetet inom en verksamhet är det viktigt att skapa en kultur där medarbetare själva ska känna att de kan kontakta en chef om behovet uppstår – till exempel om förutsättningar i privatlivet skulle kunna göra medarbetaren mer mottaglig för påtryckningar eller närmandeförsök. Uppföljningsansvaret handlar även om att säkerställa att information av betydelse för registerkontrollen fångas upp och vidarebefordras till Säkerhetspolisen, exempelvis om medarbetaren bytt tjänst och därför inte längre ska registerkontrolleras, eller förändringar i personliga förhållanden så som äktenskap eller samboförhållande.[87]

Kontinuerlig utbildning i säkerhetsskydd syftar till att säkerställa och vidmakthålla medarbetarnas kompetens inom området.[88] Förutom utbildning i övergripande säkerhetsarbete i verksamheten ska utbildning specifikt utformad för den del av verksamheten som är säkerhetskänslig ges till relevanta medarbetare. Befattningsspecifik utbildning kan även vara nödvändig för att fördjupa medarbetarnas förståelse för skyddsvärden och åtgärder kopplade till specifika arbetsuppgifter.[89]

Säkerhetsskyddslagen innefattar särskilda bestämmelser om tystnadsplikt som gäller för den som delar eller deltagit i säkerhetskänslig verksamhet samt för den som tar del av uppgifter i samband med säkerhetsprövningar. Tystnadsplikten reglerar obehörigt röjande eller utnyttjande av uppgifter som är säkerhetsskyddsklassificerade. I det allmännas verksamhet tillämpas i stället bestämmelserna i offentlighets- och sekretesslagen (2009:400).[90]

5.3 Vid avslut av deltagande i säkerhetskänslig verksamhet

Vid avslut av anställning för medarbetare som deltagit i säkerhetskänslig verksamhet är det främst två aktiviteter som ska genomföras: avslutande säkerhetssamtal och avanmälan från registerkontroll.[91]

Ett avslutande säkerhetssamtal syftar främst till att uppmärksamma om den medarbetare som slutar har eventuella missnöjen gentemot arbetsgivaren. Det avslutande samtalet bör vara strukturerat så att medarbetaren själv får möjlighet att återkoppla och komma med frågor och kan genomföras av till exempel närmsta chef eller en HR-funktion inom verksamheten. Under det avslutande samtalet är det även möjligt att påminna om tystnadsplikt, som fortsätter gälla även efter en avslutad anställning eller deltagande i en säkerhetskänslig verksamhet.

Vid avslut av anställning eller deltagande måste också registerkontroll hos Säkerhetspolisen avanmälas.

---

[87] *Säkerhetspolisen, (2023). Vägledning i säkerhetsskydd Personalsäkerhet.*

[88] *Ibid.*

[89] *Ibid.*

[90] *SFS 2018:585 Säkerhetsskyddslag*

[91] *Säkerhetspolisen, (2023). Vägledning i säkerhetsskydd Personalsäkerhet.*

6 Avslutande reflektion

Denna promemoria har tagits fram för att beskriva åtgärder kopplade till medarbetarsäkerhet som aktörer inom den finansiella sektorn kan tillämpa inom ramen för verksamheters säkerhetsarbete. Arbetet med denna typ av frågor har den senaste tiden aktualiserats på grund av den ökade hotbilden. Den ökade hotbilden är både en följd av det försämrade omvärldsläget och av kriminell verksamhet som utnyttjar finansiella funktioner för att uppnå sina syften.

För säkerhetskänslig verksamhet finns lagstiftning med tillhörande förordningar och riktlinjer som verksamheten måste efterleva och som ställer krav på arbetet med *personalsäkerhet*. Säkerhetsskyddslag (2018:585) ger verksamheten rätt att bland annat genomföra säkerhetsprövning samt löpande registerkontroll av medarbetare. Inom ramen för icke säkerhetskänslig verksamhet finns inte samma tydliga lagstiftning att ta stöd av i arbetet med säkerhetsfrågor kopplade till en verksamhets personal och medarbetare. Därför finns behov av att tydliggöra vad som bör och kan genomföras inom ramen för detta arbete, som i denna promemoria presenteras som *medarbetarsäkerhet*.

Området medarbetarsäkerhet präglas således av viss otydlighet som bland annat kommer från att kravbilden avseende vilka åtgärder och omfattningen av åtgärderna inte finns samlad. Därutöver är de krav som finns inte alltid tydliga. För att kunna fastställa en aktuell kravbild är det därför viktigt för den enskilde aktören att kartlägga vilka lagar och regelverk som påverkar denne. Det finns också en osäkerhet kring vad en arbetsgivare får göra inom ramen för medarbetarsäkerhet. Denna fråga gäller framför allt åtgärden bakgrundskontroller men också åtgärderna drogtester och uppföljande samtal. Gemensamt för bakgrundskontroller, drogtester och uppföljande samtal är att de är integritetskänsliga. För bakgrundskontroller och uppföljande samtal inom medarbetarsäkerhet finns inget specifikt lagstöd för genomförande och inte heller någon allmän definition om vad dessa bör innehålla eller hur djupt en kontroll/ett samtal ska gå.

Hur långt en verksamhet kan gå i sina åtgärder för medarbetarsäkerhet beror på flertalet faktorer. Vid genomförande av integritetskänsliga åtgärder är det av största vikt att den personliga integriteten vägs mot arbetsgivarens berättigade intresse, samt att den person som åtgärderna avser gett sitt medgivande till dem. Inom säkerhetskänslig verksamhet har avvägningen mellan personlig integritet och berättigat intresse gjorts med lagstöd när beslut fattats att den som deltar i verksamheten ska placeras i säkerhetsklass. Verksamhetens riskanalys lägger en betydande grund för allt arbete med säkerhet - medarbetarsäkerhet är inget undantag. En riskanalys genomförd med ett perspektiv på medarbetare utgör en grund för att identifiera och dimensionera åtgärder inom medarbetarsäkerhet men också ett argument för ett berättigade intresse vid exempelvis insamling av personuppgifter i samband med en bakgrundskontroll. Varje enskild aktör som arbetar med medarbetarsäkerhet behöver se över och anpassa sina åtgärder efter den egna verksamheten.

Åtgärder inom medarbetarsäkerhet som inte är integritetskänsliga, som exempelvis utbildning, interna policyer och rapporteringsvägar, genererar generellt inte samma osäkerhet som de integritetskänsliga åtgärderna. Detta är troligt på grund av att dessa åtgärder har närmare koppling till ordinarie verksamhet. Denna koppling gör dem mycket viktiga för deras inverkan på verksamhetens säkerhetskultur, vilket är en viktig aspekt i säkerhetsarbetet kopplat till medarbetare och som inte bör förbises i arbetet med medarbetarsäkerhet. Viktigt att komma ihåg i arbetet med medarbetarsäkerhet är att det inte ska begränsas till endast egna medarbetare, även

personal från leverantörer som på något sätt deltar i verksamheten bör inkluderas. Detta då de liksom de egna medarbetarna kan utgöra en sårbarhet för verksamheten, likväl som en styrka; och de bidrar också till verksamhetens säkerhetskultur.

Eftersom kärnan i medarbetarsäkerhetsfrågor är just medarbetare kan det vara bra att inkludera medarbetare och fackförbund i dialog om arbetet för att skapa en förståelse för behovet av åtgärderna. Idag finns diskussioner, ofta drivna av fackförbund, om exempelvis drogtester och bakgrundskontroller på arbetsmarknaden, i vilka frågan om personlig integritet utgör en viktig punkt. Denna typ av diskussioner kan komma påverka vad som får och inte får göras avseende denna typ av kontroller. Inom den finansiella sektorn kommer tydligare lagstöd för att genomföra bakgrundskontroller för vissa roller att komma, framför allt för de aktörer som bedriver samhällsviktig verksamhet. Frågan om åtgärder inom medarbetarsäkerhet för de som inte omfattas av de nya direktiven kommer dock att kvarstå då aktörerna inom finansiell sektor har många värden att skydda. Därför är det viktigt att aktörerna inom den finansiella sektorn fortsatt arbetar aktivt med medarbetarsäkerhet, genom att analysera krav och genomföra relevanta åtgärder.

En viktig del av arbetet med medarbetarsäkerhet är att komma ihåg att medarbetarna inte enbart utgör ett hot mot, eller en sårbarhet för, verksamheten. De är också en av verksamhetens viktigaste tillgångar i säkerhetsarbetet. En bra säkerhetskultur är ett viktigt skydd mot exempelvis möjliggörare och skapar en miljö där säkerhetsbrister och frågor kan lyftas och därmed även hanteras. En nyckel för att uppnå detta är att involvera medarbetarna, ge dem en förståelse för varför säkerhetsarbetet är viktigt och hur de kan bidra.

7 Referenser

Anförande av Carl-Oskar Bohlin, minister för civilt försvar, vid Folk och Försvars Rikskonferens 2024.

Brottsförebyggande rådet, Brå (2024). *Möjliggörare för kriminella nätverk - Om möjliggörare i kommunal, statlig och privat sektor.* Rapport 2024:2. Stockholm: Brottsförebyggande rådet.

National Insider Threat Center, (2018). *CERT Common Sense Guide to Mitigating Insider Threats*, Sixth Edition. December 2018. Technical Report CMU/SEI-2018-TR-010. Carnegie Mellon University.

Dir. 2023:30. *Genomförande av EU:s direktiv om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen och EU:s direktiv om kritiska entiteters motståndskraft*

EU:s dataskyddsförordning 2016/679 (GDPR)

Europaparlamentets och rådets direktiv (EU) 2022/2557 av den 14 december 2022 om kritiska entiteters motståndskraft och om upphävande av rådets direktiv 2008/114/EG

European Banking Authority (2024), *Final report Draft Regulatory Technical Standards to further harmonise ICT risk management tools, methods, processes and policies as mandated under Articles 15 and 16(3) of Regulation (EU) 2022/2554*

FFFS 2014:4 *Finansinspektionens föreskrifter och allmänna råd om hantering av operativa risker*

FFFS 2018:16 *Finansinspektionens föreskrifter och allmänna råd om hantering av kreditrisker i kreditinstitut och värdepappersbolag*

Försvarsmakten, (2021). *Reglemente Säkerhetstjänst*.

Integritetsmyndigheten, *Brottsuppgifter.* Hämtad: 2024-03-14

Integritetsmyndigheten, *Kan jag kräva att uppgifter om mig på Mrkoll, Eniro, Hitta.se, Lexbase, Ratsit och Merinfo tas bort?* Hämtad: 2024-04-09

Integritetsmyndigheten, *Rättslig grund.* Hämtad:2024-03-14

Integritetsmyndigheten, *Säkerhetskultur.* Hämtad: 2024-02-20.

Justitieombudsmannen (2023). Beslut 2023-10-19 dnr: 7143–2022, *Allvarlig kritik mot Kommunstyrelsen i Södertälje kommun för att i strid mot skyddet för den personliga integriteten och privatlivet ha kontrollerat om kommunanställda gjort sig skyldiga till brott*

PROP 1997/1998:97 *Polisens register*

PROP 1999/2000:123 *Lämplighetsprövning av personal inom förskoleverksamhet, skola och skolbarnsomsorg*

SFS 1991:1469 *Yttrandefrihetsgrundlagen*

SFS 1994:260 *Lagen om offentlig anställning*

SFS 1998:620 *Lagen om belastningsregister*

SFS 2010:1408 *Lag om ändring i regeringsformen*

SFS 2018:585 *Säkerhetsskyddslag*

SFS 2021:955 *Säkerhetsskyddsförordning*

SOU 2009:44 *Medicinska undersökningar – gällande regler och praxis*

SOU 2014:48 *Registerutdrag i arbetslivet*

SOU 2019:19 *Belastningsregisterkontroll i arbetslivet - behovet av utökat författningsstöd*

Svenska Bankföreningen, (2024). *Hotbildsbedömning för Sveriges Banker.*

Svenska Bankföreningen, (2023). *Säkerhet.* Hämtad: 2024-02-20.

Sveriges domstolar, *Detta blir offentligt.* Hämtad: 2024-04-09

Säkerhetspolisen, (2024). *Lägesbild 2023–2024.*

Säkerhetspolisen (2023). *Vägledning i säkerhetsskydd Fysisk säkerhet.*

Säkerhetspolisen, (2023). *Vägledning i säkerhetsskydd Informationssäkerhet.*

Säkerhetspolisen, (2023). *Vägledning i säkerhetsskydd Personalsäkerhet.*