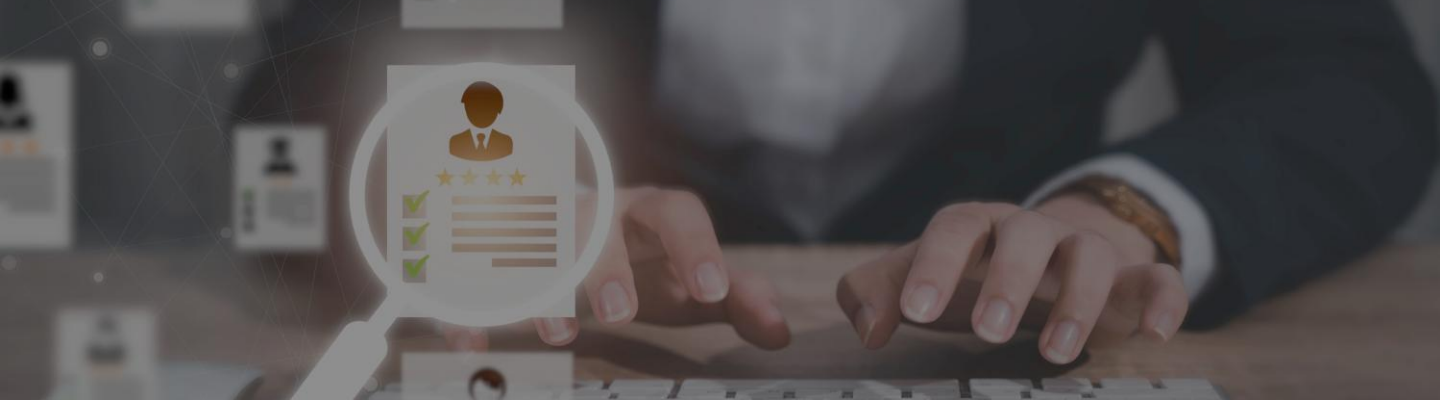
CER-direktivet

Checklista för bakgrundskontroller

För HR- och säkerhetsansvariga i organisationer som kan komma att klassas som kritiska verksamhetsutövare och omfattas av kraven på bakgrundskontroller.

Bakgrund: Utredningen om genomförande av NIS2- och CER-direktiven, SOU 2024:64

SISTEC
RIGHT TO WORK



Vad är CER-direktivet?

- Syfte: Att stärka motståndskraften hos kritiska verksamhetsutövare för att säkerställa samhällsviktiga tjänster även vid kriser, attacker eller störningar.
- Ersätter tidigare ECI-direktivet (2008/114/EG).
- Kompletterar NIS2 (cybersäkerhet) men fokuserar på fysisk och organisatorisk resiliens.
- Blir lag i Sverige genom Lagen om motståndskraft hos kritiska verksamhetsutövare (LOM)
- Kritisk verksamhetsutövare är en aktör som:
    1. Tillhandahåller samhällsviktig tjänst inom någon av de elva utpekade sektorerna.
    2. Har kritisk infrastruktur i Sverige.
    3. Där en incident kan få betydande störande effekt.

Viktiga datum

- **Årsskiftet 2025/2026:**
  Lagen om motståndskraft hos kritiska verksamhetsutövare (LOM) föreslås träda i kraft.
- **Sommaren 2026:**
  Tillsynsmyndigheter ska ha identifierat kritiska verksamhetsutövare.
- **10 månader efter identifiering:**
  Organisationer ska ha implementerat rutiner, inklusive bakgrundskontroller.

Tillsynsmyndigheter

- **MSB:s roll:** Samordnande myndighet för CER i Sverige, ansvarar för vägledning, nationell strategi och rapportering till EU.
- **Tillsynsmyndigheter:** Varje sektor får en egen tillsynsmyndighet (t.ex. Energimyndigheten för energisektorn).
- **Sanktionsavgifter:** Föreslås harmoniseras med säkerhetsskyddslagen (upp till 120 miljoner kronor, eller 2 % av global årsomsättning).

Vilka sektorer omfattas?

CER-direktivet gäller 11 kritiska sektorer:

- Energi
- Transport
- Bankverksamhet
- Infrastruktur för finansiella marknader
- Hälso- och sjukvård
- Dricksvattenförsörjning
- Avloppsvatten
- Digital infrastruktur
- Offentlig förvaltning
- Livsmedelsproduktion
- Rymdverksamhet

Verksamhetsutövare av europeisk betydelse: *Om organisationen verkar i flera EU-länder eller har gränsöverskridande påverkan, bör den bedöma om den kan klassas som verksamhetsutövare av europeisk betydelse enligt CER-direktivet. Detta kan medföra ytterligare krav på rapportering och samordning med EU-kommissionen.*

Vilka ska kontrolleras och när?

Alla med fysisk eller digital tillgång till samhällsviktig tjänst där deltagandet kan orsaka mer än ringa skada: **Anställda, konsulter och leverantörer**

Frekvens: När det finns skäl för det, men senast inom två år från senaste kontrollen

Vad ingår i en bakgrundskontroll enligt CER?

- **Säkerställd identitet:**
  Kontroll av godkänd och giltig ID-handling. Om giltighetsdatumet har passerat anses kontrollen ogiltig. ID-kontrollen är grundläggande – utan detta steg saknar övriga kontroller trovärdighet.
- **Utdrag ur belastningsregistret:**
  Den enskilde tar med ett särskilt utdrag från belastningsregistret (max 1 år gammalt) som uppvisas i samband med ID-kontrollen vid ett fysiskt möte. En anteckning om att kontrollen är gjord ska genomföras (ingen kopia eller annan information sparas).
- **Kompletterande bedömning:**
  Referenser, anställningshistorik, bedömning av lojalitet och pålitlighet, god personkännedom.
- **Ny kontroll:**
  När det finns skäl för det, men minst vartannat år.

Risker med falska identiteter

Falska ID-handlingar förekommer frekvent på arbetsmarknaden och utgör en betydande säkerhetsrisk.

För att en ID-kontroll ska anses som säker bör den alltid inkludera en äkthetsanalys av utbildad personal – enbart visuell kontroll räcker inte.

Om ID-handlingen är falsk eller ogiltig saknar övriga bakgrundskontroller trovärdighet.

Exempel på risker

- Sabotage
- Spionage
- Infiltration av kriminella
- Penningmålvakter som anställda
- Möjliggörare
- Arbetslivskriminalitet

Implementering – Steg 1 ☑

Rutiner och processer

Arbetsgivare måste dokumentera personalsäkerhetsarbetet noggrant för att möte kraven från CER. Det innebär bland annat:

- **Utse ansvarig funktion:** Utse en ansvarig för personalsäkerhet (HR-chef, säkerhetschef eller motsv.) som säkerställer att kontroller utförs enligt regelverket och att inga personer missas. Denne är också kontaktperson gentemot tillsynsmyndigheten i frågor om bakgrundskontroller.
- **Tidslinje för efterlevnad:** När organisationen har identifierats som kritisk verksamhetsutövare av tillsynsmyndigheten, har den 10 månader på sig att implementera rutiner för personalsäkerhet, inklusive bakgrundskontroller. Säkerställ att checklistan är kopplad till denna tidsfrist och att en intern projektplan finns för att möta kraven i tid.
- **Policy och rutiner:** Det ska finnas nedskrivna interna rutiner för hur bakgrundskontroller genomförs, hur ofta, av vem, och hur resultaten hanteras. Dessa dokument kan efterfrågas av tillsynsmyndigheten vid behov och är bra att ha klara för att utbilda chefer och HR-personal internt.
- **Register över kontrollerade personer:** En förteckning bör föras över vilka befattningar som identifierats som kritiska och vilka individer som innehar dem. Vidare ska man anteckna datum för utförd bakgrundskontroll per individ samt planerat datum för nästa kontroll.. Endast behörig personal ska ha åtkomst till listan.
- **Hantering av kontrollresultat:** Om en bakgrundskontroll inte ger några ”röda flaggor” räcker det oftast att notera att personen är godkänd utan anmärkning. Om det däremot framkommer något avvikande – t.ex. att registerutdraget visar en relevant dom – behöver arbetsgivaren dokumentera hur detta har hanterats. Det kan innefatta en särskild riskbedömning, beslut om eventuell omplacering eller andra åtgärder, samt att den anställde informerats och fått chans att ge sin förklaring. Även dessa steg bör journalföras.
- **Förbered för tillsyn och sanktionsrisk:** Tillsynsmyndigheter har rätt att granska rutiner, dokumentation och efterlevnad av personalsäkerhetskraven. Brister kan leda till sanktionsavgifter upp till 120 miljoner kronor eller 2 % av global årsomsättning. Säkerställ att checklistan innehåller en punkt om intern revision och att ansvariga är medvetna om tillsynsprocessen.

Implementering – Steg 2 ☑

Genomförande

- **Genomför verksamhetsbaserad riskanalys:** Innan befattningar identifieras som kritiska bör organisationen genomföra en riskbedömning av sin verksamhet. Syftet är att förstå vilka funktioner, system och roller som är mest sårbara vid incidenter. Denna analys ska dokumenteras och ligga till grund för vilka befattningar som omfattas av bakgrundskontroller.
- **Identifiera kritiska befattningar:** Genomför en *befattningsanalys* som klargör vilka tjänster i organisationen som är så betydelsefulla att en olämplig person där skulle kunna orsaka mer än ringa skada på den samhällsviktiga tjänsten. Det handlar om positioner som har stor påverkan på drift och säkerhet – t.ex. driftchefer, systemadministratörer, säkerhetsansvariga, nyckelpersonal i kontrollrum. Detta gäller även extern personal.
- **Kravställ externt:** Genomför en *befattningsanalys* av extern personal med tillgång till den samhällsviktiga tjänsten och kravställ att även denna personal ska kontrolleras. Externa aktörer ska även på begäran kunna uppvisa dokumentation som visar vilka kontroller som har blivit genomförda, när och hur.
- **Genomförande:** Utför bakgrundskontroll på personer i dessa befattningar före tillsättning (d.v.s. vid nyanställning eller intern omplacering till en sådan roll), samt löpande under anställningen. Regeringens utredningen av CER föreslår att redan anställda i kritiska roller ska kontrolleras periodiskt – minst vartannat år – för att uppmärksamma om någon tidigare pålitlig person får ändrade förhållanden som kan utgöra en risk
- **Dokumentera kontrollerna:** Ha ordnade rutiner och för register som visar att bakgrundskontroll är genomförd för varje person i de utpekade befattningarna, när den gjordes och av vem. Materialet ska kunna uppvisas vid tillsyn men i övrigt hanteras under sekretess
- **Uppföljning och påminnelse:** Implementera rutiner för notiser eller påminnelser till ansvariga för att bakgrundskontroller genomförs, som skickas i god tid innan det har gått 24 månader sedan den senaste bakgrundskontrollen för en anställd. Syftet är att säkerställa att uppföljning sker i tid och att inga kontroller missas.

Checklista ☑

- [ ] Identifiera om din organisation omfattas av CER/LOM
- [ ] Utse ansvarig för personalsäkerhetsarbetet
- [ ] Genomför riskanalys
- [ ] Kartlägg vilka roller som kräver bakgrundskontroll
- [ ] Säkerställ process för identitetsvalidering
- [ ] Upprätta register för kontroller, dokumentation och uppföljning
- [ ] Implementera digitalt stöd
- [ ] Uppdatera interna policydokument
- [ ] Utbilda personal i nya rutiner och riskmedvetenhet
- [ ] Planera för regelbundna revisioner
- [ ] Implementera rutin för intern revision
- [ ] Genomför bakgrundskontroller
- [ ] Följ upp varje kontroll vartannat år

Best practice och rekommendationer

För att hantera individkontroller som innefattar identitetsvalidering, dokumentation och uppföljning, krävs struktur och systemstöd. Både för att säkerställa att kontrollerna genomför korrekt och för att hanteringen ska ske i enlighet med gällande lagar och regler.

Sistec tjänst Right to Work erbjuder en digital plattform med automatiserade processer för att möta CER-direktivets krav på bakgrundkontroller. Sedan starten 2019 har Sistec träffat och kontrollerat över 300 000 individer på den svenska arbetsmarknaden.

Right to Work

- Äkthetsanalys av ID-handlingar
- Säkerställd identitet och nationalitet
- Kontroll av belastningsregisterutdrag i samband med ID-kontroll
- Säker dokumentation av genomförda kontroller
- Automatiserade påminnelser om uppföljning
- Möjlighet till integration med HR-system
- Kundportal för att bjuda in tredjepart (t.ex. uppdragsgivare) som behöver verifiera att leverantörens personal är kontrollerad.

Läs mer här eller kontakta oss via rtw@sistec.se