# OMVÄRLDSANALYS 2026

## Säkerhetsbranschen



Presenterad av Maja Bornefalk | Januari 2026

LEGACY

Rapporten är skriven av: Maja Bornefalk
Tel: +46 76-035 33 92
E-post: maja@legacyab.se
Om det finns några oklarheter, fel eller andra frågor som rör rapporten, vänligen kontakta Legacy AB

# Innehåll


01 Politik & Lagstiftning ..... 5
NIS2-direktivet & Cybersäkerhets-lagen ..... 6
Direkta och indirekta konsekvenser ..... 6
Krav på anpassning av erbjudande, avtal och arbetssätt ..... 6
Cyber Resilience Act ..... 7
Direkta och indirekta konsekvenser ..... 7
Krav på anpassning av produktportfölj, leverantörsstyrning och interna processer ..... 7
AI Act ..... 8
Säkerhetsskydds-lagen – ytterligare kompletteringar ..... 9
Lönetransparens-direktivet ..... 9
Transparens i rekrytering och lönesättning ..... 9
Rätt till information under anställning ..... 10
Rapportering och åtgärder vid löneskillnader ..... 10
Samlad påverkan ..... 10
02 Hållbarhet & Miljö ..... 11
CSRD ..... 12
Ett lugnare införande ..... 12
Dokumentation och livscykelkrav ..... 13
03 Ekonomi ..... 15
Köpläge och projektflöde ..... 16
Projekt och eftermarknad ..... 16
Tjänstifiering och abonnemang ..... 16
04 Digitalisering & Automation ..... 18
AI-agenter ..... 19
Ett exempel från Googles *Gemini* ..... 19
Agent i webbshoppen ..... 19
Automation i interna processer ..... 19
Smarta lås och nästa generations digital acess ..... 20
AI-baserad videoanalys & prediktiv övervakning ..... 20
Integration, mognad och ansvarsfull AI ..... 20
Reglering och vägledning ..... 21
Biometri ..... 21
Samlad innebörd ..... 21
05 Säkerhet & Försvar ..... 23

"Europe's independence moment" ..... 24
Ett skärpt omvärldsläge ..... 24
Ryssland och kriget nära EU ..... 24
USA: hårdare maktpolitik och nya friktionsytor ..... 24
Iran och regional volatilitet ..... 24
En strategisk reaktion ..... 25
Sverige: påverkan på offentlig sektor respektive privat sektor ..... 25
Offentlig sektor ..... 25
Privat sektor ..... 25
Beredskap blir affärskritiskt ..... 26
Från "krislåda" till kontinuitet, krisledning & cybersäkerhet ..... 26
*Kontinuitet i verksamheten* ..... 26
Ledningssystem som verktyg för robusthet ..... 26
06 Event & Utbildningar ..... 27
Källförteckning ..... 31

# 01
# Politik & Lagstiftning

År 2026 präglas politik och lagstiftning av ett tydligt skifte från förberedelser och inriktningsbeslut till faktisk tillämpning. Många regeländringar som beslutats under tidigare år börjar nu få konkret genomslag i form av nya skyldigheter, tydligare ansvar och ökad tillsyn. För verksamheter innebär detta att omvärldens regelkrav i större utsträckning påverkar hur arbete planeras, styrs och följs upp i praktiken.

En övergripande utveckling är att lagstiftning i allt högre grad används som styrmedel för att stärka robusthet, motståndskraft och långsiktig hållbarhet i samhället. Kraven riktas inte enbart mot slutliga resultat, utan även mot hur verksamheter organiserar sitt arbete, hanterar risker, säkerställer kontinuitet och kan visa spårbarhet i beslut och åtgärder över tid.

Samtidigt blir regelverkens påverkan mer genomgripande än tidigare. Även aktörer som inte omfattas direkt påverkas indirekt genom krav från kunder, uppdragsgivare, leverantörer och samarbetspartners. Detta gör att förmågan att förstå, omsätta och förhålla sig till förändrad lagstiftning blir en allt viktigare strategisk fråga under 2026, snarare än en isolerad juridisk eller administrativ uppgift.



# NIS2-direktivet & Cybersäkerhets-lagen

NIS2-direktivet är EU:s regelverk för att höja den gemensamma cybersäkerhetsnivån inom unionen. I Sverige genomförs direktivet genom Cybersäkerhetslagen (2025:1506), som träder i kraft den 15 januari 2026. Det innebär att NIS2 inte längre är ett kommande regelverk utan ett bindande svenskt lagkrav för de verksamhetsutövare som omfattas.[1]

Syftet med Cybersäkerhetslagen är att uppnå en hög nivå av cybersäkerhet i samhället genom att ställa krav på systematiskt och riskbaserat arbete med skydd av nätverks och informationssystem. Lagen reglerar vilka verksamheter som omfattas, vilka säkerhetsåtgärder som ska vidtas, hur incidenter ska rapporteras samt hur tillsyn och sanktioner ska tillämpas.[2]

Jämfört med läget när 2025 års omvärldsanalys togs fram innebär detta en tydlig förskjutning från osäkerhet kring införande till ett konkret regelverk med fast ikraftträdandedatum, tydliga skyldigheter för verksamhetsutövare samt möjligheter till tillsyn, förelägganden och sanktionsavgifter.[3]

## Direkta och indirekta konsekvenser

Företag i säkerhetsbranschen påverkas antingen direkt om verksamheten omfattas av Cybersäkerhetslagens kriterier, eller indirekt genom att kunder som omfattas måste ställa tydligare krav på leverantörskedjans säkerhet.
Cybersäkerhetslagen kräver att säkerhetsåtgärder minst ska omfatta säkerhet i leveranskedjan samt säkerhet vid förvärv, utveckling och underhåll av nätverks och informationssystem, vilket gör att uppkopplade säkerhetssystem behöver hanteras som en del av kundens och ibland även leverantörens cybersäkerhetsarbete.[4]

Incidentrapporteringen skärps i praktiken eftersom en betydande incident ska upplysas inom 24 timmar och därefter rapporteras enligt tidsfrister, vilket kan påverka hur drift, support och övervakning av säkerhetssystem organiseras och avtalas. Efterfrågan på intyg och dokumentation ökar normalt när regelverk kopplas till tillsyn och sanktioner, eftersom kunder behöver kunna visa att leverantörer stödjer efterlevnad inom exempelvis åtkomstkontroll, uppdateringsrutiner, säkra kommunikationer och incidenthantering. [5]

## Krav på anpassning av erbjudande, avtal och arbetssätt

Kartlägg vilka delar av erbjudandet som är nätverksanslutna och vilka data som behandlas, och koppla dem till kravområden i Cybersäkerhetslagen, särskilt leverantörskedja, åtkomstkontroll, tillgångsförvaltning och säker drift och underhåll.
Säkerställ att avtal och leveransmodeller stödjer kundernas efterlevnad, exempelvis tydliga SLA för säkerhetsuppdateringar, sårbarhetshantering, loggning, autentisering och incidentkommunikation.
Bygg en incidentprocess som klarar lagens rapporteringslogik och tidsfrister, inklusive förmåga att snabbt ge underlag till kundens rapportering och att leverera statusuppdateringar och slutrapportering vid behov.

[1] ”Cybersäkerhetslag (2025)”.
[2] ”Cybersäkerhetslag (2025)”.
[3] Regeringskansliet, ”Ett starkt skydd för nätverks- och informationssystem – en ny cybersäkerhetslag”.
[4] ”Cybersäkerhetslag (2025)”.
[5] ”Cybersäkerhetslag (2025)”; Regeringskansliet, ”Ett starkt skydd för nätverks- och informationssystem – en ny cybersäkerhetslag”.

# Cyber Resilience Act

EU:s Cyber Resilience Act (CRA) är en förordning som inför gemensamma, grundläggande cybersäkerhetskrav för produkter med digitala element, det vill säga hårdvara och mjukvara som helt eller delvis är avsedd att vara direkt eller indirekt uppkopplad mot en enhet eller ett nätverk. Förordningen är Regulation (EU) 2024/2847 och gäller direkt i alla medlemsstater utan att först behöva införas i svensk lag.[6]

CRA blir fullt tillämplig den 11 december 2027, men vissa delar börjar gälla tidigare, bland annat kapitel IV om anmälan av organ för bedömning av överensstämmelse från 11 juni 2026 och rapporteringsskyldigheter enligt artikel 14 från 11 september 2026.[7]

CRA innehåller både krav på säkerhet i produktens utformning och utveckling, samt krav på tillverkarens processer för sårbarhetshantering under den tid produkten förväntas vara i bruk, och den kopplas till marknadskontroll och efterlevnad.[8]

## Direkta och indirekta konsekvenser

Säkerhetsbranschen påverkas direkt eftersom många produkter som säljs och installeras är produkter med digitala element, exempelvis nätverkskameror, passersystem, uppkopplade lås, larm, gateways och tillhörande mjukvara och fjärrtjänster. För integratörer, installatörer och återförsäljare blir påverkan ofta indirekt men affärskritisk, eftersom upphandlare och kunder kommer kräva att portföljen består av CRA anpassade produkter med tydlig uppdateringspolicy och spårbar dokumentation, och eftersom CRA också ställer krav på ekonomiska aktörer i leveranskedjan.[9]

Utöver de formella kraven finns tydliga marknadssignaler om hur ledande aktörer positionerar sig inför CRA. Axis Communications har exempelvis erhållit BSI:s IT-Sicherheitskennzeichen för ett stort antal produkter och beskriver detta som ett steg i förberedelserna inför kommande EU-krav på cybersäkerhet för IoT-produkter. Detta ses som en tydlig first-mover-signal inom videosäkerhet.[10]
ASSA ABLOY beskriver på motsvarande sätt hur deras IoT-säkerhetsprogram och certifikathantering är utformade för att möta växande regulatoriska krav, inklusive den kommande Cyber Resilience Act. Detta indikerar att livscykelhantering, identitet och certifikat blir centrala konkurrensfaktorer i säkerhetsplattformar.[11]

Flera branschaktörer bedömer dessutom att kombinationen av NIS2 och CRA kommer att driva konsolidering inom säkerhetsbranschen. Enligt Seriline riskerar mindre och tekniskt svagare aktörer att slås ut när kraven på processmognad, dokumentation och kontinuerligt säkerhetsunderhåll ökar, vilket kan förändra konkurrensbilden och påskynda professionalisering i branschen.[12]

## Krav på anpassning av produktportfölj, leverantörsstyrning och interna processer

Inför en portföljstyrning där det blir standard att kunna visa leverantörernas CRA relevanta underlag, exempelvis uppdaterings och

[6] *Cyberresiliensförordningen (EU) 2024/2847*.
[7] "The Cyber Resilience Act - Summary of the Legislative Text | Shaping Europe's Digital Future".
[8] *Cyberresiliensförordningen (EU) 2024/2847*.
[9] *Cyberresiliensförordningen (EU) 2024/2847*.
[10] "Axis erhält IT-Sicherheitskennzeichen des BSI | Axis Communications"; Bundesamt für Sicherheit in der Informationstechnik, "BSI erteilt IT-Sicherheitskennzeichen an Axis Communications GmbH".
[11] "ASSA ABLOY Strengthens IoT Security".
[12] SecurityWorldMarket.com, "Seriline".

supportpolicy, sårbarhetsrutiner, teknisk dokumentation och hur produkten ska konfigureras säkert i drift.
Ställ tydligare krav på leverantörer i inköp och avtal, så att ni kan få snabb information om sårbarheter, uppdateringar och rekommenderade motåtgärder, eftersom CRA skärper kraven på sårbarhetshantering och spårbarhet över tid.
Bygg en intern rutin för hur produktrelaterade sårbarheter och incidenter ska fångas upp och eskaleras mot leverantör och kund, så att ni kan stötta kunder som vill dokumentera att de hanterar risker i sin leveranskedja och sin drift. [13]

Undvik att hamna i oavsiktligt tillverkaransvar genom att ha kontroll på när en förändring i en lösning kan bedömas som en väsentlig ändring av en produkt, och dokumentera tydligt vad som är produktens ursprungliga avsedda användning och vad som är integration och konfiguration.[14]

# AI Act

EU:s AI-förordning, vanligen kallad AI Act, är världens första heltäckande regelverk för artificiell intelligens och trädde i kraft den 1 augusti 2024. De flesta bindande kraven börjar dock tillämpas först från den 2 augusti 2026, vilket innebär att påverkan på verksamheter successivt kommer att öka under perioden 2026–2027.[15]

AI Act bygger på ett riskbaserat angreppssätt där AI-system delas in i förbjuden AI, hög-risk-AI samt begränsad eller minimal risk. För säkerhetsbranschen är hög-risk-kategorin särskilt relevant, eftersom den omfattar flera tillämpningar som redan används eller är på väg att införas i branschen.[16]

Hög-risk-AI inkluderar bland annat biometrisk identifiering, AI-baserad analys i kamerabevakning, samt AI-system som används för skydd av kritisk infrastruktur, exempelvis för intrångsdetektion, riskanalys eller automatiserad övervakning. Även realtidsbaserad fjärridentifiering med ansiktsigenkänning i offentliga miljöer är som huvudregel förbjuden enligt AI Act, med endast mycket snäva undantag för brottsbekämpande myndigheter.

För leverantörer av sådana AI-system innebär hög-risk-klassificeringen omfattande krav, bland annat på riskhantering, dokumentation av hela AI-systemets livscykel, datakvalitet, loggning, mänsklig tillsyn samt konformitetsbedömning innan system får tas i bruk.[17]

Även säkerhetsföretag i rollen som deployer, det vill säga de som installerar eller driver AI-baserade system åt kund, omfattas av krav på korrekt användning enligt leverantörens instruktioner, mänsklig övervakning samt rapportering av allvarliga incidenter.[18]

Trots att AI Act ännu inte är en central diskussionsfråga inom den svenska säkerhetsbranschen innebär regelverket att AI-baserade säkerhetslösningar i praktiken blir en regulatorisk fråga snarare än enbart en teknisk eller affärsmässig fråga. Tillsammans med NIS2-direktivet, som ställer krav på riskhantering, incidentrapportering och ledningsansvar för nätverks- och informationssystem, samt Cyber Resilience Act (CRA), som fokuserar på säkerhet i produkter med digitala element över hela livscykeln, bidrar AI Act till ett samlat regelverkstryck på säkerhetsbranschen. Sammantaget pekar detta mot att aktörer som arbetar med kamerabevakning, biometriska lösningar och AI-baserad analys behöver förhålla sig till flera överlappande regelverk från 2026 och framåt, där teknisk säkerhet, regelefterlevnad och affärsstrategi i allt högre grad hänger ihop.

[13] *Cyberresiliensförordningen (EU) 2024/2847*.
[14] "Cyber Resilience Act - Proposal for a Regulation".
[15] "AI Act Enters into Force - European Commission".
[16] *Annex III*.
[17] *EU Artificial Intelligence Act | Up-to-Date Developments and Analyses of the EU AI Act*.
[18] *Article 26*.

# Säkerhetsskydds-lagen – ytterligare kompletteringar

SOU 2025:42 *Säkerhetsskyddslagen – ytterligare kompletteringar* presenterades i april 2025 och innehåller förslag på skärpningar och förtydliganden av säkerhetsskyddslagen (2018:585). Utredningen har tagits fram mot bakgrund av det försämrade säkerhetspolitiska läget och ett ökat behov av att skydda säkerhetskänslig verksamhet, samhällsviktig funktionalitet och kritiska leveranskedjor i Sverige.[19]

För säkerhetsbranschen är förslagen relevanta eftersom företag ofta agerar leverantörer till säkerhetskänslig verksamhet, exempelvis kommuner, regioner, statliga myndigheter eller kritisk infrastruktur.

Utredningen tydliggör att tillsyn inte enbart ska kunna riktas mot den offentliga eller privata verksamhetsutövaren, utan även mot leverantören i ett pågående samarbete. Det innebär att säkerhetsföretag kan bli föremål för tillsyn, krav eller förelägganden om deras roll bedöms kunna påverka Sveriges säkerhet.

Vidare innebär den föreslagna anmälningsplikten att kunder kan behöva anmäla samarbeten med säkerhetsföretag även när säkerhetsskyddsavtal inte formellt krävs. Detta kan leda till ökad granskning av leverantörers rutiner, personal, informationshantering och tekniska lösningar.

För branschen innebär detta ett ökat behov av att kunna visa ordning och reda i säkerhetsarbetet, tydliga roller i uppdrag samt förståelse för säkerhetsskyddslagstiftningens krav.[20]

# Lönetransparens-direktivet

EU:s lönetransparensdirektiv (Directive (EU) 2023/970) antogs i maj 2023 och syftar till att stärka principen om lika lön för kvinnor och män för lika eller likvärdigt arbete genom ökad transparens, tydligare rättigheter för arbetstagare och skärpta krav på arbetsgivare. Direktivet är en del av EU:s bredare jämställdhets- och arbetsmarknadspolitik och får genomslag i samtliga branscher och sektorer. Medlemsstaterna ska ha genomfört direktivet i nationell lagstiftning senast den 7 juni 2026.[21]

## Transparens i rekrytering och lönesättning

En central förändring är att transparens ska införas redan före anställning. Arbetsgivare ska informera arbetssökande om ingångslön eller löneintervall för den aktuella tjänsten, exempelvis i platsannons eller senast inför intervju. Samtidigt förbjuds arbetsgivare att efterfråga uppgifter om en kandidats tidigare lönehistorik.
Syftet är att motverka att historiska löneskillnader förs vidare och att skapa mer

[19] Regeringskansliet, ”Säkerhetsskyddslagen – ytterligare kompletteringar”.
[20] Sverige, *Säkerhetsskyddslagen*.
[21] Directive (EU) 2023/970 of the European Parliament and of the Council of 10 May 2023 to Strengthen the Application of the Principle of Equal Pay for Equal Work or Work of Equal Value between Men and Women through Pay Transparency and Enforcement Mechanisms (Text with EEA Relevance); Regeringskansliet, ”Genomförande av lönetransparensdirektivet”.

jämlika förutsättningar i rekryteringsprocessen.[22]

## Rätt till information under anställning

Direktivet ger arbetstagare rätt att begära information om genomsnittliga lönenivåer, uppdelade på kön, för grupper av arbetstagare som utför samma eller likvärdigt arbete.
Detta ställer krav på att arbetsgivare kan ta fram tillförlitlig och jämförbar lönedata baserad på objektiva och könsneutrala kriterier, samt har rutiner för hur sådan information lämnas ut.

## Rapportering och åtgärder vid löneskillnader

För större organisationer införs krav på regelbunden lönerapportering, där rapporteringsskyldighet och intervall beror på organisationens storlek. Arbetsgivare med 150–249 anställda ska lämna sin första rapport senast den 7 juni 2027, och därefter vart tredje år.
Om rapporteringen visar ett löneskillnadsgap över 5 procent som inte kan förklaras med könsneutrala kriterier uppstår en skyldighet att vidta åtgärder, exempelvis genom gemensam lönebedömning tillsammans med arbetstagarrepresentanter.

Mindre organisationer omfattas inte av krav på formell lönerapportering, men berörs ändå av direktivets grundläggande krav. De ska kunna redogöra för hur löner sätts, säkerställa att löneskillnader kan motiveras med objektiva och könsneutrala kriterier samt hantera förfrågningar om löneinformation från arbetstagare. Vid identifierade osakliga löneskillnader förväntas även mindre arbetsgivare vidta korrigerande åtgärder, även om någon rapporteringsskyldighet inte föreligger.[23]

## Samlad påverkan

Lönetransparensdirektivet innebär att lönefrågor i ökande grad blir en styrnings- och regelefterlevnadsfråga snarare än enbart en personaladministrativ fråga. Kraven driver behov av tydligare strukturer för lönesättning, rekrytering och uppföljning i verksamheter inom alla branscher.

[22] Consilium, ”Pay Transparency in the EU”.

[23] Consilium, ”Pay Transparency in the EU”.

# 02
# Hållbarhet & Miljö

År 2026 kännetecknas hållbarhets- och miljöområdet av att långsiktiga mål och politiska ambitioner i allt högre grad omsätts i konkreta krav, styrmedel och förväntningar på verksamheter. Utvecklingen drivs både av formella regeländringar och av ökade krav från offentliga aktörer, marknaden och andra intressenter, vilket gör att hållbarhet blir en mer integrerad del av ordinarie verksamhetsstyrning.

En tydlig trend under 2026 är att fokus flyttas från övergripande ambitioner till mätbarhet, spårbarhet och genomförande. Miljö- och hållbarhetsfrågor kopplas allt oftare till dokumentation, uppföljning och livscykelperspektiv, där verksamheter förväntas kunna visa hur påverkan hanteras över tid – inte bara i planering, utan även i drift, leverans och förvaltning.

Samtidigt breddas påverkan. Även aktörer som inte omfattas av direkta krav påverkas indirekt genom upphandlingar, kundkrav, värdekedjor och samverkansformer. Detta gör att hållbarhet och miljö 2026 i ökande grad blir en strategisk fråga som påverkar konkurrenskraft, resursanvändning och långsiktigt handlingsutrymme, snarare än ett avgränsat sidospår eller ett separat projekt.



# CSRD

Hållbarhetsrapportering har blivit ett lagkrav i Sverige genom EU:s nya direktiv (CSRD), där de har valts att införa direktivet på miniminivå och där det stegvis omfattar fler företag från 2024 och framåt.

Det innebär att större företag måste redovisa detaljerad hållbarhetsinformation i årsredovisningen, medan mindre företag i dagsläget inte omfattas direkt, utan påverkas främst via värdekedjan. För dessa aktörer är det dock klokt att arbeta strukturerat redan nu, exempelvis genom ett

miljöledningssystem som ISO 14001, eftersom det både underlättar framtida rapportering och gör det lättare att möta ökade kundkrav innan rapporteringsplikten eventuellt utvidgas.

## Ett lugnare införande

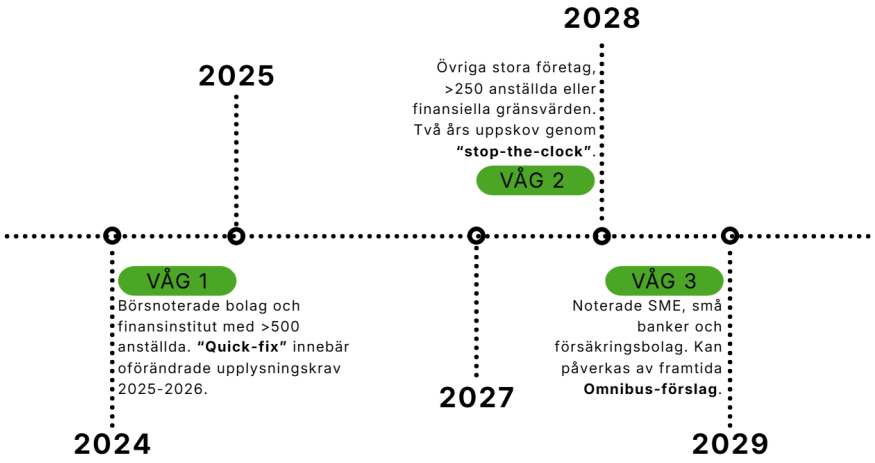
Under 2025 har tre viktiga EU-beslut

förändrat förutsättningarna för CSRD och inneburit ett mer stegvis och mindre belastande införande än vad som ursprungligen planerades.

För det första antogs det så kallade ”stop-the-clock”-direktivet (EU) 2025/794[24], som skjuter upp rapporteringskraven med två år för företag som annars skulle ha omfattats från räkenskapsår 2025 (våg 2) och 2026 (våg 3). Syftet är att ge företag mer tid att bygga upp processer, systemstöd och datainsamling.

För det andra antog EU-kommissionen i juli 2025 en ”quick-fix”-delegerad akt[25], som innebär att företag i våg 1 inte behöver lämna fler eller mer detaljerade upplysningar under räkenskapsåren 2025 och 2026 än vad som redan krävdes för 2024. Rapporteringen fryses därmed tillfälligt på samma nivå, vilket minskar den administrativa belastningen i ett tidigt skede.

För det tredje presenterade EU-kommissionen i februari 2025 ett Omnibus-förslag[26], där inriktningen är att på sikt fokusera CSRD på de allra största företagen (över 1 000 anställda) och samtidigt minska indirekta rapporteringskrav på mindre leverantörer. Förslaget är ännu inte beslutat, men ses av många marknadsaktörer som en tydlig signal om att EU vill begränsa rapporteringsbördan för SME.




*Figur 1: CSRD – införande i vågor (uppdaterat läge efter EU-beslut 2025. Figuren visar när olika företagskategorier omfattas av CSRD samt hur införande för våg 2 och 3 har senarelagts. För våg 1 gäller tillfälligt oförändrade rapportering krav under 2025-2026.*

Sammantaget innebär detta att kraven på CSRD delvis har lättats eller förskjutits, även om rapporteringsplikten i grunden ligger fast. För små och medelstora företag innebär det att de har mer tid att förbereda sig, och att ett strukturerat miljöarbete, till exempel via ISO 14001, är ett rimligt sätt att ligga steget före både kommande regler och kundernas ökade krav.

[24] Directive (EU) 2025/794 of the European Parliament and of the Council of 14 April 2025 Amending Directives (EU) 2022/2464 and (EU) 2024/1760 as Regards the Dates from Which Member States Are to Apply Certain Corporate Sustainability Reporting and Due Diligence Requirements (Text with EEA Relevance).

[25] ”Commission Adopts “Quick Fix” for Companies Already Conducting Corporate Sustainability Reporting - Finance”.

[26] ”Omnibus Package - European Commission”.

# Dokumentation och livscykelkrav

Intressenternas miljökrav mot säkerhetsbranschen rör sig snabbt från ”ambition” till bevisbar produkt- och livscykeldata.

EU har infört ESPR för att driva fram mer hållbara produkter (t.ex. längre livslängd, reparerbarhet, resurseffektivitet) och för att standardisera vilken information som ska följa produkten.[27]

I praktiken blir Digital Product Passport (DPP) det ”nya kvittot” på miljöprestanda och spårbarhet, ett sätt att få data att flöda mellan aktörer för at möjliggöra cirkuläret och kontroll[28], vilket gör att kunder lättare kan ställa skarpa krav i upphandling och avtal.

För säkerhetsbranschen påverkar detta ofta indirekt. Även om man inte tillverkar, kan man behöva visa eller överlämna produktdata (till exempel DPP-länk/ID, material- och serviceinformation) för det komponenter man installerar, byter ut, eftersom införandet nu går in i en mer konkret fas genom EU-kommissionens arbetsplan 2025-2030.[29]

På sikt förstärks livcykelfokuset ytterligare eftersom produktpasset enligt svensk myndighetsinformation ska vara tillgängligt inte bara för köpare och myndigheter, utan även för aktörer vid slutet av livscykeln (till exempel återvinnare), vilket kan öka trycket på tydliga rutiner för returflöden, utbyten och hantering av utrangerad utrustning i serviceaffären.[30]

[27] ”EU-förordningen om ekodesign för hållbara produkter (ESPR)”.
[28] Jonsson, *EU och digitala produktpass (DPP)*.
[29] ”2025-2030 Working Plan - Green Forum - European Commission”.
[30] ”Ekodesignförordningen”.

# DIN PARTNER I EN FÖRÄNDERLIG OMVÄRLD

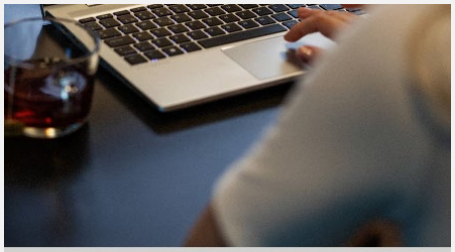
Hos Legacy hittar du expertstöd, utbildningar och verksamhetsnära lösningar som är relevanta när regler, risker och krav förändras. Kontakta oss för att staka ut er väg framåt i en osäker värld.



## Legacy Core

**Verksamhetsutveckling** →

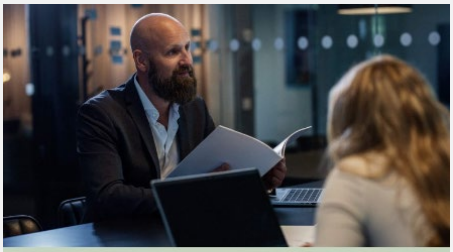
Experter på ledningssystem, certifieringar, processkartläggningar, Six Sigma och implementering av Lean.



## Legacy Shield

**Person- & informationssäkerhet** →

Skyddar bolag och myndigheter genom grundutredning för säkerhetskänslig verksamhet vid t ex rekryteringar och konsultuppdrag.



## Legacy Learn

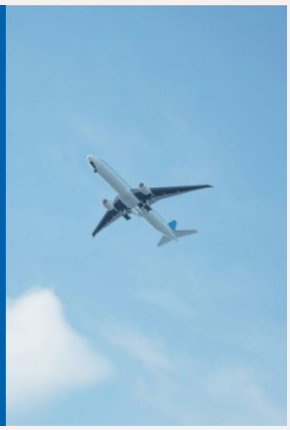
**Utbildningar** →

Grundläggande Arbetsmiljöutbildning och Grundläggande Miljöutbildning för säker arbetsmiljö och ökad hållbarhet.

## Legacy Air

**Luftvärdighetsgranskning** →

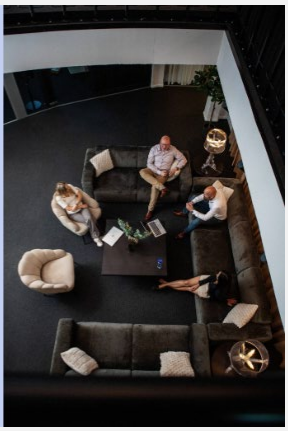
Genom luftvärdighetsgranskning säkerställer vi att flygplan uppfyller kraven enligt EASA Part-M Subpart I.



## Legacy Lead

**Genomförandekraft** →

Seniora ledare/chefer som interimslösningar vid stora eller oväntade förändringar när organisationen behöver stöttning.



KONTAKTA OSS ⟶ Se hur vi kan hjälpa er framåt ⟶

legacyab.se | info@legacyab.se

LEGACY

# 03
# Ekonomi

År 2026 präglas det ekonomiska läget av en gradvis stabilisering efter flera år av hög inflation, snabba ränteförändringar och ökad osäkerhet. Även om inflationen har dämpats och ränteläget i många prognoser bedöms vara mer stabilt, kvarstår osäkerhet kring konjunkturens riktning, investeringsvilja och offentliga finanser. Detta skapar ett ekonomiskt klimat där både privata och offentliga aktörer blir mer selektiva i sina prioriteringar.

En tydlig utveckling under 2026 är att ekonomiska beslut i allt högre grad kopplas till krav, risk och långsiktig effektivitet. Investeringar som kan motiveras genom regelkrav, robusthet, minskad sårbarhet eller tydliga effektivitetsvinster prioriteras framför mer långsiktiga eller svårmätbara nyttor. Samtidigt ökar kraven på att insatser ska vara skalbara, återanvändbara och möjliga att följa upp över tid.

Marknadsläget kännetecknas också av ökade skillnader mellan segment, regioner och affärsmodeller. Projekt- och investeringsdrivna delar av ekonomin påverkas ofta snabbare av konjunktursvängningar, medan verksamheter med återkommande intäkter, service, eftermarknad eller abonnemangsbaserade upplägg tenderar att uppvisa större motståndskraft. För många aktörer blir därför balans mellan kortsiktig försiktighet och långsiktig positionering en central ekonomisk fråga under 2026.

Sammantaget innebär detta att ekonomi 2026 inte enbart handlar om kostnadsnivåer och tillväxt, utan om hur resurser styrs, prioriteras och används mer strategiskt i en omvärld där marginaler, krav och förväntningar är tydligare än tidigare.



# Köpläge och projektflöde

Under 2026 pekar många prognoser på lägre inflation och en styrränta som kan ligga still, men med osäkerhet kring när nästa skifte kommer.[31]

En stor del av branschen följer nybyggnation, ROT och ombyggnation. Prognoser pekar på att installationsvolymerna kan växa även 2026. där kommunikations- och säkerhetsteknik bedöms öka (om än i lugnare takt än vissa andra delområden). Det betyder: fler projekt igen, men fortsatt prispress och hård konkurrens om lönsamheten i projektleveranser.[32]

# Projekt och eftermarknad

I den här miljön syns en tydlig skillnad mellan projektberoende affärer och återkommane/uppgraderingsdriven efterfrågan.

ASSA ABLOY beskriver en stark utveckling i utmanande marknad och lyfter att deras exponering mot aftermarket ger motståndskraft, med stark efterfrågan på uppdrageringar till elektronmechaniska och digitala lösningar även när delar av marknaden är mjukare.[33]

Samtidigt visar installationsnära aktörer som Bravida hur konkurrensen och prispressen i projekt slår: de beskriver ett läge där de blivit mer restriktiva i projektval och fokusera på marginal, med stabil orderstock men utmaningar i kassaflöde kopplat till stora projekt och faktureringsvillkor. Bravida lyfter även tydliga skillnader i Norden: Sverige är fortsatt utmanande (med stora geografiska skillnader), där försäljningen minskat och projektmixen förskjutits mot fler installationsprojekt med något lägre marginal, vilket pressat EBITA, där det nu har påbörjats en översyn av den svenska organisationenen för bättre styrning och effektivitet. Samtidigt beskrivs Danmark som positivt med tydligt förbättrad lönsamhet (EBITA 2025 nära 5 %), Norge stabiliserar marginalen via hög andel service, och Finland är fortsatt tufft men med åtgärder och orderstock som väntas stödja förbättring framåt.[34]

Internationellt speglar dormakaba ettliknande mönster. Resultat som förbättras via kostnadskontroll men svagare efterfrågan i vissa segment, bl.a. residential, och osäkerhet kopplat till handel/tullar, men ändå med förvänta om fortsatt organisk tillväxt framåt.[35]

# Tjänstifiering och abonnemang

I den mer tjänstifierade delen av säkerhetsmarknaden signalerar Verisure en stark utveckling i årliga återkommande intäkter (ARR) och uttrycker fortsatt förtroende för sin tillväxt[36]. Deras modell bygger på att ”Portfolio Services” levererar en professionellt övervakad säkerhetstjänst mot en månadsvis abonnemangsavgift (24/7-övervakning, verifieirng/åtgärd, kundservice, underhåll och teknisk support), där de normalt tecknar självförnyande övervakningsavtal i samband med installation.[37] De betonar också att en lojal kundbas med låg bortfall ger förutsägbara

[31] *Penningpolitisk rapport december 2025.*
[32] Installatörsföretagen, ”Installationstrender hösten 2025”.
[33] *Quarterly Report Q2 2025.*
[34] Bravida, ”Interim Report July–September 2025”.
[35] ”Dormakaba to pass on tariff costs to customers as it targets North American growth | Reuters”.
[36] ”Verisure Reports Results for Q3 2025”.
[37] *Verisure plc Interim Report January - September 2025.*

kassaflöden, och att de återkommande månadsavgifterna står för cirka 85 procent av omsättningen (2024).[38] Sammantaget stödjer det bilden att abonnemangsmodeller ofta är mer konjunkturstabila än ren installationsförsäljning.

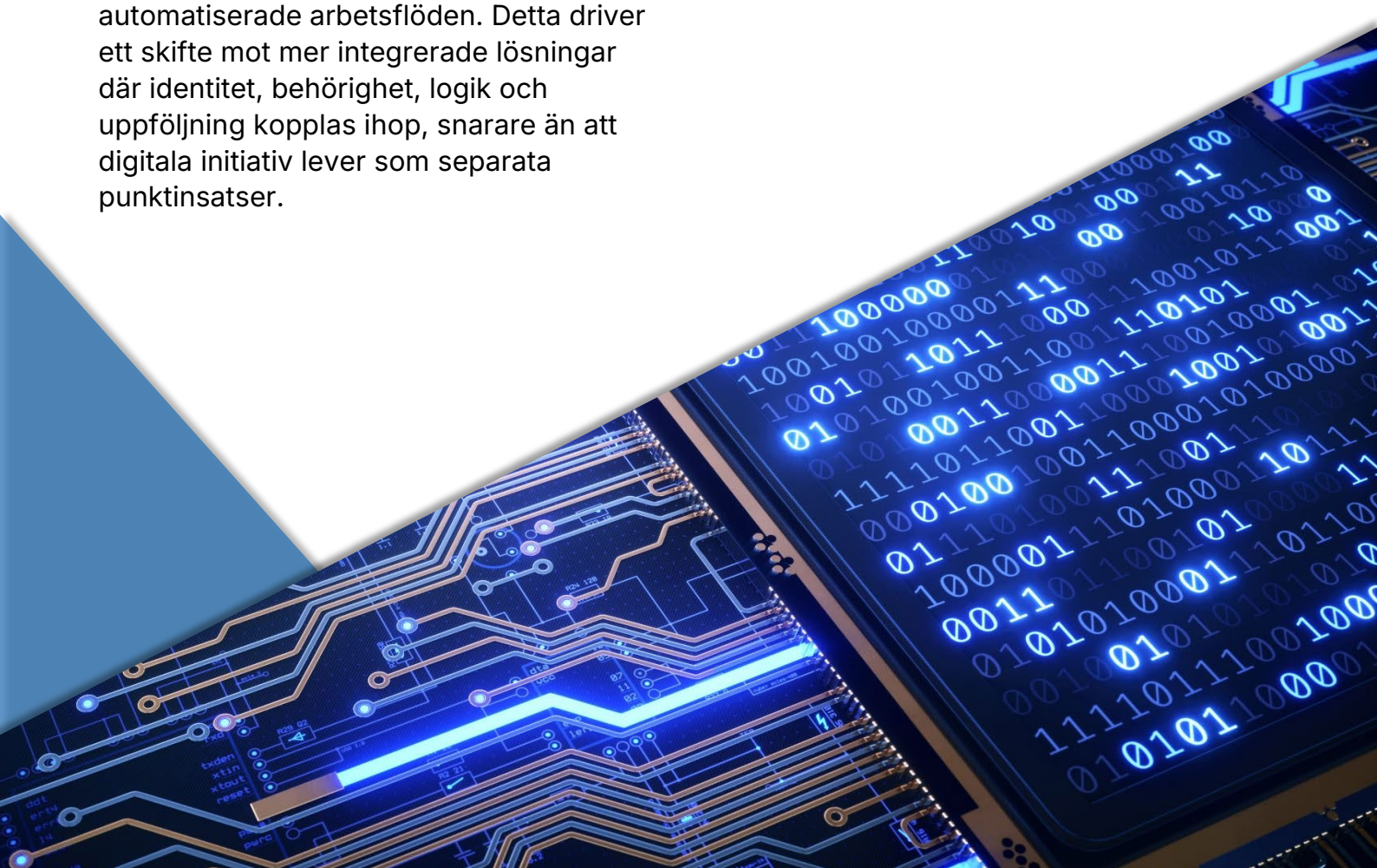
[38] *Verisure Midholding AB Annual Report 2024*.

# 04
# Digitalisering & Automation

År 2026 ser vi att digitalisering och automatisering går in i en mer mogen fas där fokus flyttas från enskilda verktyg och piloter till hur teknik faktiskt skapar effekt i kärnverksamheten. Förväntningarna ökar på att digitala satsningar ska ge mätbar nytta i form av högre produktivitet, bättre styrning, kortare ledtider och minskad administration, samtidigt som kraven på kontroll, spårbarhet och ansvarsfull användning blir tydligare.

En central utveckling under 2026 är att data blir mer ”operativt”: information ska kunna återanvändas mellan system, flöden och aktörer, och fungera som underlag för både beslut och automatiserade arbetsflöden. Detta driver ett skifte mot mer integrerade lösningar där identitet, behörighet, logik och uppföljning kopplas ihop, snarare än att digitala initiativ lever som separata punktinsatser.

Samtidigt blir digitalisering i ökande grad en samverkansfråga. Verksamheter som standardiserar hur de väljer användningsfall, inför teknik, hanterar risker och delar fungerande lösningar får snabbare utväxling än de som utvecklar isolerat. Sammantaget gör detta att digitalisering och automation 2026 handlar mindre om ”ny teknik” och mer om genomförandeförmåga: struktur, styrning och arbetssätt som gör att tekniken kan skalas och ge långsiktig effekt.



# AI-agenter

AI-agenter (”agentic AI”) är AI-system som kan utföra uppgifter mot ett mål genom att planera steg, hämta information, använda verktyg (t.ex. sök, databaser, API:er), och i vissa fall initiera åtgärder i andra system (t.ex. skapa ärenden, uppdatera data, föreslå/verkställa nästa steg). Det som skiljer en agent från en vanlig chattbot är att den inte bara svarar, den kan driva ett flöde och agera inom givna ramar.[39]

## Ett exempel från Googles *Gemini*

En kund besöker en webbplats och beskriver ett problem, till exempel att en växt inte mår bra. Den digitala agenten ber om tillgång till kameran för att kunna se växten och tolkar det som syns,exempelvis bladens skick, jorden och krukan. Därefter ställer agenten relevanta följdfrågor om ljusförhållanden och vattningsrutiner. Utifrån informationen kan agenten också uppmärksamma att kunden har valt fel typ av jord eller näring i varukorgen och istället rekommendera rätt alternativ, direkt kopplat till butikens sortiment och aktuella lagerstatus. Agenten kan sedan guida kunden vidare hela vägen till köp.[40] Denna typ av ”visa mig”-stöd liknar funktioner som Googles Gemini Live, där användaren kan dela kamera eller skärm för att få hjälp i realtid med det man tittar på.[41]

Google har visat hur Gemini kan kopplas till en webbutiks produktdata (RAG) för att hitta rätt bland många artiklar, jämföra alternativ och guida användaren i köpresan – ett typiskt agentmönster: behov → sök i katalog → föreslå → nästa steg.[42]

## Agent i webbshoppen

En AI-agent på företagets webbplats kan ge mer exakt vägledning än en vanlig chattbot genom att (med rätt behörigheter och integritetsinställningar) använda kundens *kontext*: tidigare köp, kompatibla tillbehör, garantiinformation, vad som redan ligger i varukorgen, leveransadress, samt produktdata och lagerstatus. Agenten kan då agera som en “digital butiksspecialist” som både minskar felköp och höjer konverteringen, t.ex.:

Jag har redan lagt två produkter i korgen – saknas något för att det ska fungera?” → agenten flaggar kompatibilitet, rätt fästen/adapter, installationsmaterial, eller föreslår ett paket.

“Jag vill ha samma som förra gången men i större mängd” → agenten hittar senaste beställningen och föreslår uppskalad variant.

## Automation i interna processer

Inköp, projektadministration, dokumenthantering, avvikelseflöden, offertunderlag och statusrapportering kan bli agentdrivna, men ställer högre krav på datakvalitet, behörigheter och uppföljning eftersom agenten kan påverka riktiga arbetsflöden. Riskytan förändras dock när agenter får åtkomst till verktyg och systemintegrationer. Då blir risken inte bara att agenter ger fel svar, utan att den faktiskt kan utföra felaktiga åtgärder, hantera behörigheter på ett osäkert sätt eller påverkas av manipulerad indata. Dessa risker hamnar närmare kärnverksamheten och behöver därför hanteras genom tydliga kontrollpunkter, genomtänkta behörighetsnivåer och säkra designval.

[39] Gemini, ”Gemini Agent - AI Automation for Daily Tasks & Multi-Step Work”; Google Cloud, ”The AI Agent Handbook”.
[40] AI CATALYST, *Google’s new AI Agent demo. Identifies plants from video you share on spot. Recommends product#ai.*
[41] Davis, ”Google Is Rolling out Gemini’s Real-Time AI Video Features”.
[42] ”An Online Shopping Demo with Gemini and RAG | Google Cloud Blog”.

# Smarta lås och nästa generations digital acess

Utvecklingen av smarta lås rör sig från enklare appstyrda lösningar mot mer automatiserade och identitetsbaserade system där smarta telefoner och smartklockor fungerar som primära digitala nycklar. En viktig möjliggörare är Ultra Wideband (UWB), som genom hög precision i både avstånd och riktning möjliggör säker hands free-upplåsning och minskar risken för obehörig åtkomst jämfört med äldre tekniker.[43]

Denna teknikutveckling förstärks av Aliro, en gemensam standard framtagen av Apple, Google och Samsung, som syftar till att göra mobila enheter till universella digitala nycklar oberoende av lås- och plattformsleverantör. Standardiseringen väntas påskynda marknadsadoptionen och driva ett skifte från produktfokus till plattformsbaserad digital access.[44]

Övergången från fysiska RFID-kort och brickor till mobilbaserade identiteter beskrivs av branschaktörer som en redan etablerad trend. Mobil access bedöms vara både mer användarvänlig och enklare att administrera för organisationer, samtidigt som den möjliggör ökad integration mellan passersystem, smarta byggnader och andra säkerhetssystem.[45]

Sammantaget innebär utvecklingen att digital identitet, automatiserad åtkomst och systemintegration blir allt viktigare konkurrensfaktorer inom säkerhetsbranschen. Detta driver på både teknisk modernisering och ett gradvis skifte bort från traditionella RFID-lösningar.

# AI-baserad videoanalys & prediktiv övervakning

Utvecklingen inom kamera- och sensor system går snabbt från tradtionell ”bildsamling” till AI-baserad tolkning i relatid, där system kan klassificera händelser/objekt, skapa smart metadata och ge operatörer ett mer prioriterat larmflöde. Det driver ett skifte från reaktiv övervakning till mer förutseende och automatiserad incdienthantering, där AI fungerar som ett beslutsstöd som minskar bruset och frigör tid för operatörer och bevakningsersurser.[46]

Svenska och Sverige-nära aktörer beskriver detta som en tydlig 2026-trend. Securitas Techology lyfter AI (tillsammans med molnapplikation och avancerade sensorer, som även var en trend för 2025) som en av de mest centrala teknikrörelserna för 2026, och pekar på att utvecklingen går mot mer prediktiva arbetssätt.[47]

## Integration, mognad och ansvarsfull AI

Axis Communications beskriver i sin rapport, om AI i videoövervakning, hur AI används för att stärka säkerhet och trygghet, men också för operativ effektivitet och “business intelligence”, samtidigt som ansvarsfull AI (integritet, etik, risk för missbruk) blir allt mer avgörande när kapaciteten ökar.[48]

[43] Tuohy, ”Hands-on with Hands-Free Unlocking”.
[44] CSA-IOT, ”Aliro”.
[45] Barton, ”Security Technology Trends 2026 #2”.
[46] *The state of AI in video surveillance*; Vd och Sverige, ”Trendrapporten 2026”.
[47] *2026 års rapport om globala tekniktredner*.
[48] *The state of AI in video surveillance*.

En viktig del av mognaden 2026 och framåt handlar också om integration. AI-analys blir mer värdefull när den kopplas ihop med andra säkerhets- och fastighetssystem (t.ex. VMS, larmflöden och händelsehantering) så att "larm" blir en del av ett automatiserat arbetsflöde snarare än en enskild notis.[49]

## Reglering och vägledning

Samtidigt blir 2026 extra relevant eftersom reglering och vägledning för AI och biometri konkretiseras, vilket påverkar hur lösningar kan designas och säljas. EU-kommissionen har publicerat riktlinjer om förbjudna AI-praktiker enligt AI-förordningen, och riktlinjerna tar bland annat upp realtids fjärrbiometrisk identifiering och andra förbjudna tillämpningar.[50]

I Sverige har riksdagen dessutom beslutat om ändringar som utökar möjligheterna till kamerabevakning och förenklar förfarandet i offentlig verksamhet, bland annat genom att ta bort tillståndskravet för kamerabevakning för offentliga aktörer samt ge brottsbekämpande myndigheter bättre möjligheter i fler miljöer och i brådskande fall.[51]

## Biometri

När det gäller biometri blir den främst relevant som en del av "nästa steg" i identitets- och verifieringskedjan, särskilt i högre skyddsnivåer och i miljöer där man vill minska risken för delade behörigheter och förbättra spårbarhet. Här behöver man dock hålla isär olika användningsfall: autentisering/inpassering i en kontrollerad miljö är något annat än biometrisk identifiering på allmän plats. IMY är tydlig med att ansiktsigenkänning bygger på behandling av biometriska uppgifter och att GDPR därför måste följas när tekniken utvecklas eller används. IMY lyfter också särskilt vad som gäller i arbetslivet för arbetsgivares behandling av biometriska personuppgifter (t.ex. ansiktsigenkänning och fingeravtryck), vilket i praktiken gör rättslig grund, proportionalitet och skyddsåtgärder till centrala krav vid införande. [52]

Svensk samhällsdebatt och myndighetslinje visar samtidigt att biometrisk fjärridentifiering på allmän plats är en högintegritetskänslig fråga. DO har exempelvis avstyrkt förslag som skulle möjliggöra AI-baserad ansiktsigenkänning/biometrisk fjärridentifiering i realtid på allmän plats för brottsbekämpande ändamål, även om DO samtidigt uttrycker förståelse för behovet av åtgärder mot grov organiserad brottslighet.[53]

## Samlad innebörd

AI-videoanalys och intelligenta övervakningsflöden blir en allt viktigare konkurrensfaktor (bättre larmkvalitet, snabbare respons, mer automatiserad drift), men 2026 och framåt blir också ett läge där leveransförmåga inkluderar styrning och efterlevnad d.v.s. tydliga ändamål, dataminimering, åtkomstkontroller, loggning och korrekt hantering av biometriska tillämpningar där de används.

[49] *The state of AI in video surveillance*.
[50] "Commission Publishes the Guidelines on Prohibited Artificial Intelligence (AI) Practices, as Defined by the AI Act. | Shaping Europe's Digital Future".
[51] Regeringskansliet, "Regeringen går vidare med lagförslag om utökad kamerabevakning".
[52] "Integritetsskyddsmyndigheten | IMY"; "Integritetsskyddsmyndigheten | IMY".
[53] "Polisens användning av AI för ansiktsigenkänning i realtid"; Regeringskansliet, "Remiss av promemorian Polisens användning av AI för ansiktsigenkänning i realtid (Ds 2025".


LEGACY
Ditt Legacy Vårt Legacy.

# 05
# Säkerhet & Försvar

År 2026 präglas säkerhets- och försvarsområdet av ett mer allvarligt och oförutsägbart omvärldsläge, där gränsen mellan fred, kris och höjd beredskap blivit mindre tydlig. Säkerhetspolitik, ekonomi, teknik och samhällsfunktioner hänger allt tätare ihop, vilket gör att robusthet och handlingsförmåga får en mer central roll i både offentlig och privat verksamhet.

En tydlig utveckling under 2026 är att säkerhet och försvar inte längre ses som avgränsade statliga frågor, utan som något som berör hela samhället. Förmågan att upprätthålla samhällsviktiga funktioner, hantera störningar och verka under osäkra förhållanden blir en gemensam angelägenhet där ansvar, beroenden och roller mellan aktörer behöver fungera även under press.

Samtidigt rör sig fokus från övergripande strategier och planer till mer konkret genomförande. Beredskap förväntas i allt högre grad vara operativ, uthållig och integrerad i ordinarie styrning, snarare än något som hanteras vid sidan av. Det innebär ett ökat behov av tydliga arbetssätt, samverkan och strukturer som gör det möjligt att agera snabbt, prioritera rätt och följa upp förmåga över tid.

Sammantaget gör detta att säkerhet och försvar 2026 blir en strategisk fråga för hur verksamheter planerar, organiserar och samverkar i en mer osäker omvärld – med fokus på kontinuitet, ansvarstagande och praktisk motståndskraft snarare än enbart reaktiva åtgärder.



# ”Europe’s independence moment”

Von der Leyens ”Europe’s Independence Moment” är i grunden ett budskap om handlingsfrihet, att Europa ska kunna ta större ansvar för egen säkerhet och försvar, minska strategiska beroenden inom teknik och energi, och samtidigt vara öppet men mer selektivt i partnerskap, för att ”bestämma vår egen framtid”. [54]

I praktiken syns detta i att EU parallellt driver mer gemensam försvarsförmåga och snabbare industrikapacitet, bland annat via initiativ som knyter ihop finansiering, gemensamma projekt och leverasförmåga. Ett konkret exempel är EU:s arbete med EDIP (European Defence Industry Programme), som syftar till att stärka europeisk försvarsindustriell beredskap och kapacitet.[55]

## Ett skärpt omvärldsläge

EU:s “independence”-retorik blir mer konkret när omvärlden visar hur snabbt spelregler kan ändras – genom krig i Europas närområde, gråzonsangrepp, energipåverkan, och mer oförutsägbara geopolitiska drag som påverkar handel, råvaror, sjöfart och teknikflöden.[56]

## Ryssland och kriget nära EU

SOTEU 2025 placerar Rysslands krig och hotbilden nära EU:s gränser i centrum (bl.a. incidenter med ryska drönare mot/över Polen som exempel på eskalation nära NATO-territorium). Detta är en “när-omvärld” som gör att EU:s försvars- och resiliensagenda får tydligare brådska.[57]

## USA: hårdare maktpolitik och nya friktionsytor

Under vintern 2025/2026 har USA:s agerande i västvärlden och närområden lyft frågor om territorium, råvaror och sanktionspolitik som direkt kan spilla över på europeiska intressen.

En uppdaterad översikt från US Congress (CRS) beskriver en skärpt amerikansk linje med sanktioner/åtgärder kopplade till Venezuelas oljehandel och politiska utveckling, vilket belyser hur snabbt energi och geopolitik kan bli säkerhetsfrågor som påverkar marknader och leveranskedjor.[58]

Händelser vid Davos i januari 2026 visar hur Grönland (säkerhet, mineraler och baser) blivit en tydligare geopolitisk friktionsyta mellan USA och europeiska allierade, där NATO-diplomati och europeiska reaktioner hamnar i fokus.[59]

## Iran och regional volatilitet

Samtidigt pekar nya analyser/rapportering på att instabilitet kring Iran kan bära nukleära och regionala spridningsrisker, vilket i sin tur kan påverka global risknivå, energimarknader och sjöfart.[60] IAEA:s rapportspår visar att kärnfrågan fortsatt är en central parameter i omvärldsrisken, även när läget skiftar snabbt.[61]

[54] ”State of the Union 2025 - European Commission”.
[55] Consilium, ”Programmet för europeisk försvarsindustri”.
[56] ”State of the Union 2025 - European Commission”.
[57] News, ”NATO Downs Russian Drones over Poland after ’unprecedented’ Aggression”; ”State of the Union 2025 - European Commission”.
[58] ”Venezuela”.
[59] AP News, ”NATO Chief Mark Rutte’s Shows He’s the ’Trump Whisperer’ after Greenland Diplomacy with Trump”.
[60] español, ”Analysts Warn That Iran Crisis Carries Potential Nuclear Risks”.
[61] ”IAEA and Iran - IAEA Board Reports”.

### En strategisk reaktion

Samlat blir "Europe's Independence Moment" inte bara ett politiskt motto utan en strategisk reaktion på en omvärld där säkerhet, ekonomi och teknik hänger ihop, och där Europas och Sveriges robusthet i hög grad avgörs av hur väl offentlig och privat sektor kan planera, samverka och leverera även under störning.

# Sverige: påverkan på offentlig sektor respektive privat sektor

I svensk kontext blir EU-linjen i praktiken en del av totalförsvarsuppbyggnadnen, där roller och beroenden mellan offentlig och privat sektor behöver fungera även under störningar.

### Offentlig sektor

SKR lyfter att Sveriges säkerhet och motståndskraft bygger på ett starkt civilt försvar och en god krisberedskap i kommuner och regioner.[62]

Samtidigt pekar SKR i ett yttrande på ett tydligt problem i gränslandet privat–offentligt: behovet av att tydligare reglera privata leverantörers ansvar för att upprätthålla samhällsviktig verksamhet vid fredstida kriser och höjd beredskap. Det är en viktig "översättningspunkt" i din analys: offentliga verksamheter är ofta beroende av privata leverantörer, och robusthet måste byggas i både drift och avtal.[63]

### Privat sektor

Svenskt Näringsliv driver linjen att företagen är centrala i svensk beredskap och att ett mer osäkert omvärldsläge och Nato-medlemskapet ställer ökade krav, men också skapar nya villkor, för företagen.[64]

För försvars- och säkerhetsnära företag blir EU:s industrisatsningar också ett mer direkt spår. SOFF (branschorganisationen) välkomnar kommissionens EDIP-förslag och beskriver det som ambitiöst med flera konkreta åtgärder, i vilket man kan dra slutsatsen att "Independence Moment" inte bara är retorik, utan också regel- och programutveckling som påverkar industrins villkor.[65]

För bygg- och installationsföretag blir utvecklingen mer konkret genom att regeringen infört en ny beredskapssektor för industri, byggande och handel (med Tillväxtverket som sektorsansvarig och Boverket som beredskapsmyndighet), vilket signalerar att fler företag i byggkedjan förväntas bidra till försörjningstrygghet vid störningar.[66] Samtidigt pekar SOU 2025:68 på att Boverket och MCF ska snabbspåra under 2026 hur förstärkningsresurser för byggnads- och reparationsberedskap kan utformas och finansieras.[67] Byggföretagen uppmanar redan nu företag att börja förbereda sig för uppdrag vid höjd beredskap.[68]

[62] "Regionens arbete med kris-beredskap och civilt försvar".
[63] "Krisberedskapsaspekter i offentliga kontrakt".
[64] Cervantes, "Näringslivet har en avgörande roll i totalförsvaret".
[65] *Remissvar avseende kommissionens förordningsförslag om inrättandet av det europeiska försvarsindustriprogrammet (EDIP) 2024 0061 (COD) - SOFF*.
[66] Regeringskansliet, "Nya beredskapssektorer ska stärka Sveriges civila försvar".
[67] Regeringskansliet, "Nya samverkansformer, modern byggnads- och reparationsberedskap".
[68] Byggföretagen, "Beredskap".

# Beredskap blir affärskritiskt

Sverige har de senaste åren växlat upp totalförsvarstänket – men det som är nytt nu är att företagen tydligare lyfts in som en avgörande del av motståndskraften. Under 2024 uppdaterades och skickades broschyren ”Om krisen eller kriget kommer” ut till hushållen.

Nästa steg kom i början av 2026: en motsvarighet riktad till företag, *”Beredskap för företag – Om krisen eller kriget kommer”*. Broschyren är framtagen av Myndigheten för civilt försvar (MCF) och är ett komplement till hushållsbroschyren från 2024.[69]

Samtidigt har MSB genomgått ett tydligt skifte i identitet och inramning. Från 1 januari 2026 är Myndigheten för civilt försvar (MCF)[70], ett namnbyte som ska betona rollen som nationell nod för civilt försvar och samordning inför kris, höjd beredskap och krig.
Tillsammans med nytt material riktat till företag blir bilden tydligare: beredskap handlar inte enbart om offentliga aktörer och hushåll, utan även om att verksamheter kan upprätthålla kritiska funktioner.

## Från ”krislåda” till kontinuitet, krisledning & cybersäkerhet

I företagsbroschyren är budskapet rakt: vid kris eller krig har svenska företag “en avgörande roll” för att samhället ska fortsätta fungera, och den viktigaste insatsen är ofta att upprätthålla verksamheten så långt det är möjligt.[71]

Broschyren paketerar råden i tydliga fokusområden, Några områden som är särskilt viktiga för många organisationer är:

*Kontinuitet i verksamheten*
Kontinuitetshantering lyfts som ett centralt verktyg: kartlägg vad som måste fungera, identifiera beroenden (personal, el, transporter), analysera leverantörer och försörjningskedjor och stärk robustheten med praktiska åtgärder som reservkraft, lagerhållning och reservrutiner

*Krishanteringsförmåga*
En uppdaterad krisplan och en krisorganisation med tydliga roller (ledning, kommunikation, lägesbild, personal, leveranser, drift, säkerhet) och kontaktvägar är grundläggande. Broschyren trycker också på att skriva ut kontaktlistor, säkra alternativa kontaktvägar och öva regelbundet.

*Systematiskt cybersäkerhetsarbete*
Här är kopplingen till risk- och konsekvensbedömning extra tydlig: arbeta systematiskt och riskbaserat, dokumentera risker, konsekvenser och säkerhetsåtgärder – och bygg grundhygien som MFA, uppdateringar och offline-backuper.

## Ledningssystem som verktyg för robusthet

Ett ledningssystem (standarder, processer och tydliga roller) hjälper organisationer att göra beredskap praktisk och styrbar. Det skapar struktur för att prioritera vad som är kritiskt, fördela ansvar, arbeta riskbaserat och följa upp åtgärder över tid. På så sätt blir kontinuitet, krisledning och säkerhetsarbete inte en engångsinsats, utan en del av ordinarie styrning som kan övas, förbättras och anpassas när omvärldsläget förändras.

[69] ”Beredskap för företag”.
[70] ”MSB är Myndigheten för civilt försvar”.
[71] ”Beredskap för företag”.

# 06
# Event & Utbildningar

Detta kapitel samlar exempel på event, konferenser och utbildningar som kan vara relevanta under 2026. Urvalet omfattar både återkommande och mer tillfälliga aktiviteter och speglar områden där utvecklingen går snabbt, där nya krav växer fram eller där erfarenhetsutbyte och omvärldsbevakning är särskilt värdefullt.

Syftet med sammanställningen är att ge en överblick över möjliga arenor för kompetensutveckling, nätverkande och fördjupad förståelse för omvärldens förändringar. Event och utbildningar fyller ofta en viktig funktion genom att knyta samman regelutveckling, teknikskiften och praktisk tillämpning, samt genom att skapa mötesplatser mellan verksamheter, branscher och beslutsfattare.

Relevansen av de enskilda aktiviteterna varierar beroende på verksamhetens uppdrag, mognad och aktuella prioriteringar. Vissa kan fungera som strategisk omvärldsbevakning på ledningsnivå, medan andra är mer operativa och inriktade på konkreta arbetssätt, metoder eller kompetenshöjning. Sammanställningen ska därför ses som ett stöd för planering och prioritering under året, snarare än som en fullständig eller bindande lista.



**SSG Säkerhetskonferens** – *18–19 mars 2026, Quality Hotel Globe (Stockholm)*
Tvådagarskonferens som passar för den som vill vet mer om säkerhetsläge, robusthet, incidenter och ledningens ansvar.

Arrangör: SSG[72]

**Fastighetsdagen Göteborg** – *15 april 2026, Elite Park Avenue Hotel, Göteborg*
Seminarium med starkt fastighetsfokus (inkl. trygghet/uthyrning/utveckling). Bra för installatörer och säkerhetsleverantörer som vill möta fastighetsägare/beslutsfattare och fånga upp behov kopplat till passersystem, trygghet och fastighetsutveckling.[73]

**Branddagarna 2026** – *23–24 april 2026, The Steam Hotel (Västerås)*
Praktiskt inriktad konferens för brandskydd/säkerhet/teknik.

Arrangör: Securitas Technology[74]

**Bostadsbrandskonferensen 2026** – *6–7 maj 2026, Stockholm*
Arrangeras av bl.a. Myndigheten för civilt försvar/Brandforsk/Brandskyddsföreningen. Relevant för trygghet, brandskydd och riskreducering i bostadsbestånd.

Arrangörer: MCF, Brandforsk, Brandskyddsföreningen[75]

**SäkerhetsDagen 2026** – *21 maj 2026, Münchenbryggeriet (Stockholm)*
Blandar samhällssäkerhet/totalförsvar, organiserad brottslighet och cybersäkerhet – bra "nav-event" i en omvärldsanalys för säkerhetssektorn.

Arrangör: Säkerhetsbranschen[76]

**SKYDD** – *20–22 oktober 2026, Stockholmsmässan*
Större nordisk mässa för safety & security, räddning och personskydd. Bra om du har teknikskiften, integrerade lösningar och leverantörsmarknad som tema.[77]

**Säkerhetsdagen** – *1 december 2026*
Renodlad informations- och cybersäkerhetsdag Arrangör: Certezza[78]

**Elmia Subcontractor –** *10–12 nov 2026, Jönköping*
Underleverantörs- och industrimötesplats. Bra för prospektering och för att fånga upp krav som drivs i leverantörskedjor[79]

**Trygg & Säker** – *25–26 november 2026, Clarion Hotel & Congress Sea U, Helsinborg*
Konferens/mötesplats för trygghet, brottsförebyggande arbete, krisberedskap och civilt försvar. Bra för aktörer som jobbar mot offentlig sektor/fastigheter och vill förstå behov och knyta kontakter.[80]

**Grundläggande Arbetsmiljöutbilndning (SAM)** – (e-learning). Introduktion till arbetsmiljö och systematiskt arbetsmiljöarbete (SAM), med praktiska verktyg som SAM-hjulet, riskbedömning, åtgärdstrappan samt uppföljning av tillbud/incidenter. Avslutas med kunskapstest och diplom. Riktad till medarbetare.

Arrangör: Legacy[81]

**Grundläggande Miljöutbildning** – (e-learning). Översikt över hållbar utveckling och företagsnära miljöarbete, med inslag om

[72] "SSG Säkerhetskonferens".
[73] Wredenmark, "Fastighetsdagen Göteborg | Fastighetsvärlden".
[74] "Branddagarna 2026 | Securitas Technology".
[75] *Bostadsbrandskonferensen 2026 | 6–7 maj 2026 · Stockholm*.
[76] "Årets stora säkerhetshändelse".
[77] "SKYDD October 20-22 2026".
[78] "Säkerhetsdagen".
[79] Elmia, "Elmia Subcontractor | Heart of industrial know-how".
[80] "Trygg & Säker - Trygg & Säker".
[81] "Arbetsmiljöutbildning (SAM)".

Miljöbalkens principer, ansvar kopplat till kemikalier/avfall, miljöriskbedömningar samt introduktion till miljöledningssystem (MLS).
Arrangör: Legacy[82]

**Sectech Sweden** – *26–27 oktober 2027, Stockholm*
Nordisk säkerhetsmässa med tydligt teknikfokus (lås, passersystem, inbrottslarm, CCTV, integrerade säkerhetslösningar och leverantörsmarknad). Bra för att fånga upp produktnyheter, systemintegrationer och trender i installationsledet samt knyta kontakter med tillverkare, distributörer och slutkunder.[83]

[82] ”Grundläggande Miljöutbildning För Företag”.
[83] ”SECTECH Sweden”.

# Legacy Insights

Vill ni hålla er uppdaterade även mellan årets analyser?

På **Legacy Insights** delar vi löpande insikter, tolkningar och praktiska perspektiv på förändringar inom lagstiftning, säkerhet, cybersäkerhet och verksamhetsstyrning.

- → Kvalitet & ledningssystem
- → Lagstiftning, krav & säkerhet
- → Digitalisering, AI & framtida arbetssätt

Insikter mellan årets analyser →

legacyab.se | info@legacyab.se

LEGACY

# Källförteckning


1. ”2025-2030 Working Plan - Green Forum - European Commission”. Åtkomstdatum 14 januari 2026. https://green-forum.ec.europa.eu/news/2025-2030-working-plan-2025-07-11_en.

2. *2026 års rapport om globala tekniktredner*. Securiats Technology, u.å. Åtkomstdatum 22 januari 2026. https://reports.securitastechnology.com/view/557354365/.

3. ”AI Act Enters into Force - European Commission”. Åtkomstdatum 07 januari 2026. https://commission.europa.eu/news-and-media/news/ai-act-enters-force-2024-08-01_en.

4. AI CATALYST. *Google’s new AI Agent demo. Identifies plants from video you share on spot. Recommends product#ai*. 2025. 04:42. https://www.youtube.com/watch?v=_HQNDF-GBVg.

5. ”An Online Shopping Demo with Gemini and RAG | Google Cloud Blog”. Åtkomstdatum 28 januari 2026. https://cloud.google.com/blog/products/ai-machine-learning/an-online-shopping-demo-with-gemini-and-rag.

6. *Annex III: High-Risk AI Systems Referred to in Article 6(2) | EU Artificial Intelligence Act*. u.å. Åtkomstdatum 07 januari 2026. https://artificialintelligenceact.eu/annex/3/.

7. AP News. ”NATO Chief Mark Rutte’s Shows He’s the ’Trump Whisperer’ after Greenland Diplomacy with Trump”. 22 januari 2026. https://apnews.com/article/rutte-nato-trump-greenland-aaeec48ee94881ffd838a66d85e92c2e.

8. ”Arbetsmiljöutbildning (SAM)”. *Legacy*, u.å. Åtkomstdatum 26 januari 2026. https://www.legacyab.se/courses/arbetsmiljoutbildning/.

9. *Article 26: Obligations of Deployers of High-Risk AI Systems | EU Artificial Intelligence Act*. u.å. Åtkomstdatum 07 januari 2026. https://artificialintelligenceact.eu/article/26/.

10. ”ASSA ABLOY Strengthens IoT Security”. Åtkomstdatum 05 januari 2026. https://www.assaabloy.com/group/en/news-media/stories/access-stories/assa-abloy-strengthens-iot-security.

11. ”Axis erhält IT-Sicherheitskennzeichen des BSI | Axis Communications”. 24 mars 2025. https://newsroom.axis.com/de-de/press-release/axis-bsi-it-security-label.

12. Barton, Jaroslav. ”Security Technology Trends 2026 #2: Jaroslav Barton, HID Global”. 02 januari 2026. Webb-TV / videointervju. https://www.securityworldmarket.com/se/Webb-TV/security-technology-trends-2026-2-jaroslav-barton-hid-global.

13. ”Beredskap för företag : Om krisen eller kriget kommer”. Åtkomstdatum 22 januari 2026. https://www.mcf.se/sv/publikationer/beredskap-for-foretag--om-krisen-eller-kriget-kommer/.

14. *Bostadsbrandskonferensen 2026 | 6–7 maj 2026 · Stockholm*. u.å. Åtkomstdatum 26 januari 2026. https://bostadsbrand.se/.

15. ”Branddagarna 2026 | Securitas Technology”. Åtkomstdatum 26 januari 2026. https://www.securitastechnology.com/sv/branddagarna.

16. Bravida. ”Interim Report July–September 2025”. 24 oktober 2025. https://www.bravida.se/en/press/press-releases/2025/interim-report-julyseptember-2025/.

17. Bundesamt für Sicherheit in der Informationstechnik. ”BSI erteilt IT-Sicherheitskennzeichen an Axis Communications GmbH”. Åtkomstdatum 05 januari 2026. https://www.bsi.bund.de/DE/Service-Navi/Presse/Alle-Meldungen-News/Meldungen/IT-Sik_Axis_250324.html?nn=520690.

18. Byggföretagen. ”Beredskap”. Åtkomstdatum 22 januari 2026. https://byggforetagen.se/beredskap/.

19. Cervantes, Skriven avGabriel Cardona. ”Näringslivet har en avgörande roll i totalförsvaret”. Svenskt Näringsliv. Åtkomstdatum 22 januari 2026. https://www.svensktnaringsliv.se/sakomraden/sakerhet-och-risk/naringslivet-har-en-nyckelroll-i-totalforsvaret_1207153.html.

20. ”Commission Adopts “Quick Fix” for Companies Already Conducting Corporate Sustainability Reporting - Finance”. Åtkomstdatum 12 januari 2026. https://finance.ec.europa.eu/publications/commission-adopts-quick-fix-companies-already-conducting-corporate-sustainability-reporting_en.

21. ”Commission Publishes the Guidelines on Prohibited Artificial Intelligence (AI) Practices, as Defined by the AI Act. | Shaping Europe’s Digital Future”. Åtkomstdatum 22 januari 2026. https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-prohibited-artificial-intelligence-ai-practices-defined-ai-act.

22. Consilium. ”Pay Transparency in the EU”. Åtkomstdatum 29 januari 2026. https://www.consilium.europa.eu/en/policies/pay-transparency/.

23. Consilium. ”Programmet för europeisk försvarsindustri: rådet och parlamentet når preliminär överenskommelse”. Åtkomstdatum 22 januari 2026. https://www.consilium.europa.eu/sv/press/press-releases/2025/10/16/european-defence-industry-programme-council-and-parliament-reach-provisional-agreement/.

24. CSA-IOT. ”Aliro”. Åtkomstdatum 07 januari 2026. https://csa-iot.org/all-solutions/aliro/.

25. ”Cyber Resilience Act - Proposal for a Regulation”. *Cyber Resilience Act*, u.å. Åtkomstdatum 05 januari 2026. https://www.cyberresilienceact.eu/the-cyber-resilience-act/.

26. ”Cybersäkerhetslag (2025:1506)”. Åtkomstdatum 05 januari 2026. https://www.riksdagen.se/sv/dokument-och-lagar/dokument/svensk-forfattningssamling/cybersakerhetslag-20251506_sfs-2025-1506/.

27. Davis, Wes. ”Google Is Rolling out Gemini’s Real-Time AI Video Features”. The Verge, 23 mars 2025. https://www.theverge.com/news/634480/google-gemini-live-video-screen-sharing-astra-features-rolling-out.

28. Directive (EU) 2025/794 of the European Parliament and of the Council of 14 April 2025 Amending Directives (EU) 2022/2464 and (EU) 2024/1760 as Regards the Dates from Which Member States Are to Apply Certain Corporate Sustainability Reporting and Due Diligence Requirements (Text with EEA Relevance), EP, CONSIL (2025). http://data.europa.eu/eli/dir/2025/794/oj.

29. Directive (EU) 2023/970 of the European Parliament and of the Council of 10 May 2023 to Strengthen the Application of the Principle of Equal Pay for Equal Work or Work of Equal Value between Men and Women through Pay Transparency and Enforcement Mechanisms (Text with EEA Relevance), EP, CONSIL, 132 OJ L (2023). http://data.europa.eu/eli/dir/2023/970/oj.

30. ”Dormakaba to pass on tariff costs to customers as it targets North American growth | Reuters”. Åtkomstdatum 15 januari 2026. https://www.reuters.com/technology/dormakaba-pass-tariff-costs-customers-it-targets-north-american-growth-2025-09-02/.

31. ”Ekodesignförordningen”. Åtkomstdatum 14 januari 2026. https://www.energimyndigheten.se/effektiv-energianvandning/saljare-och-tillverkare-av-produkter/ekodesign-energimarkning-och-ce-markning/ekodesign/ekodesignforordningen/.

32. Elmia. ”Elmia Subcontractor | Heart of industrial know-how”. Åtkomstdatum 26 januari 2026. https://www.elmia.se/subcontractor/.

33. español, STEPHANIE LIECHTENSTEIN Leer en. ”Analysts Warn That Iran Crisis Carries Potential Nuclear Risks”. AP News, 19 januari 2026. https://apnews.com/article/iran-nuclear-material-theft-sabotage-142a84ea137b38306d58829be29dbe39.

34. *EU Artificial Intelligence Act | Up-to-Date Developments and Analyses of the EU AI Act*. u.å. Åtkomstdatum 07 januari 2026. https://artificialintelligenceact.eu/.

35. ”EU-förordningen om ekodesign för hållbara produkter (ESPR)”. Åtkomstdatum 14 januari 2026. https://www.naturvardsverket.se/amnesomraden/cirkular-ekonomi/eu-forordningen-om-ekodesign-for-hallbara-produkter-espr/.

36. *Europaparlamentets och rådets förordning (EU) 2024/2847 av den 23 oktober 2024 om övergripande cybersäkerhetskrav för produkter med digitala element och om ändring av förordningarna (EU) nr 168/2013 och (EU) 2019/1020 och direktiv (EU) 2020/1828 (cyberresiliensförordningen) (Text av betydelse för EES)*. u.å.

37. Gemini. ”Gemini Agent - AI Automation for Daily Tasks & Multi-Step Work”. Åtkomstdatum 28 januari 2026. https://gemini.google/overview/agent/.

38. Google Cloud. ”The AI Agent Handbook”. Åtkomstdatum 28 januari 2026. https://cloud.google.com/resources/content/ai-agent-handbook.

39. ”Grundläggande Miljöutbildning För Företag”. *Legacy*, u.å. Åtkomstdatum 26 januari 2026. https://www.legacyab.se/courses/grundlaggande-miljoutbildning/.

40. ”IAEA and Iran - IAEA Board Reports”. Text. IAEA, 29 juli 2014. http://www.iaea.org/newscenter/focus/iran/iaea-and-iran-iaea-board-reports.

41. Installatörsföretagen. ”Installationstrender hösten 2025”. Åtkomstdatum 14 januari 2026. https://www.in.se/aktuellt/rapporter/Installationstrender/installationstrender-hosten-2025/.

42. ”Integritetsskyddsmyndigheten | IMY”. Åtkomstdatum 22 januari 2026. https://www.imy.se/verksamhet/dataskydd/dataskydd-pa-olika-omraden/arbetsliv/biometri/.

43. ”Integritetsskyddsmyndigheten | IMY”. Åtkomstdatum 22 januari 2026. https://www.imy.se/verksamhet/dataskydd/innovationsportalen/vagledning-om-ansiktsigenkanning-och-gdpr/gdpr-och-ansiktsigenkanningsteknik/.

44. Jonsson, Christina. *EU och digitala produktpass (DPP)*. u.å.

45. ”Krisberedskapsaspekter i offentliga kontrakt”. Åtkomstdatum 22 januari 2026. https://www.upphandlingsmyndigheten.se/upphandla-till-samhallsviktig-verksamhet/krisberedskapsaspekter-i-offentliga-kontrakt/.

46. ”MSB är Myndigheten för civilt försvar”. Åtkomstdatum 22 januari 2026. https://www.mcf.se/sv/om-oss/vart-uppdrag/msb-ar-myndigheten-for-civilt-forsvar/.

47. News, A. B. C. ”NATO Downs Russian Drones over Poland after ’unprecedented’ Aggression”. ABC News. Åtkomstdatum 22 januari 2026. https://abcnews.go.com/International/poland-airspace-repeatedly-violated-drone-type-objects-amid/story?id=125422386.

48. ”Omnibus Package - European Commission”. Åtkomstdatum 12 januari 2026. https://finance.ec.europa.eu/news/omnibus-package-2025-04-01_en.

49. *Penningpolitisk rapport december 2025*. u.å.

50. ”Polisens användning av AI för ansiktsigenkänning i realtid”. Text. Åtkomstdatum 22 januari 2026. https://www.do.se/om-do/vad-arbetar-do-med/remissvar/2025/2025-06-09-polisens-anvandning-av-ai-for-ansiktsigenkanning-i-realtid.

51. *Quarterly Report Q2 2025*. 2025. https://www.assaabloy.com/group/en/documents/investors/interim-reports/2025/Q2%20Report%202025.pdf.

52. Regeringskansliet, Regeringen och. ”Ett starkt skydd för nätverks- och informationssystem – en ny cybersäkerhetslag”. Text. Regeringskansliet, Regeringen och Regeringskansliet, 14 oktober 2025. https://doi.org/10/prop.-20252628.

53. Regeringskansliet, Regeringen och. ”Genomförande av lönetransparensdirektivet”. Text. Regeringskansliet, Regeringen och Regeringskansliet, 29 maj 2024. https://www.regeringen.se/rattsliga-dokument/statens-offentliga-utredningar/2024/05/sou-202440/.

54. Regeringskansliet, Regeringen och. ”Nya beredskapssektorer ska stärka Sveriges civila försvar”. Text. Regeringskansliet, Regeringen och Regeringskansliet, 26 juni 2025. https://www.regeringen.se/pressmeddelanden/2025/06/nya-beredskapssektorer-ska-starka-sveriges-civila-forsvar/.

55. Regeringskansliet, Regeringen och. ”Nya samverkansformer, modern byggnads- och reparationsberedskap”. Text. Regeringskansliet, Regeringen och Regeringskansliet, 09 juni 2025. https://www.regeringen.se/rattsliga-dokument/statens-offentliga-utredningar/2025/06/sou-202568/.

56. Regeringskansliet, Regeringen och. ”Regeringen går vidare med lagförslag om utökad kamerabevakning”. Text. Regeringskansliet, Regeringen och Regeringskansliet, 03 februari 2025. https://www.regeringen.se/pressmeddelanden/2025/02/regeringen-gar-vidare-med-lagforslag-om-utokad-kamerabevakning/.

57. Regeringskansliet, Regeringen och. ”Remiss av promemorian Polisens användning av AI för ansiktsigenkänning i realtid (Ds 2025:7)”. Text. Regeringskansliet, Regeringen och Regeringskansliet, 20 mars 2025. https://www.regeringen.se/remisser/2025/03/remiss-av-promemorian-polisens-anvandning-av-ai-for-ansiktsigenkanning-i-realtid-ds-20257/.

58. Regeringskansliet, Regeringen och. ”Säkerhetsskyddslagen – ytterligare kompletteringar”. Text. Regeringskansliet, Regeringen och Regeringskansliet, 11 april 2025. https://www.regeringen.se/rattsliga-dokument/statens-offentliga-utredningar/2025/04/sou-202542/.

59. ”Regionens arbete med kris-beredskap och civilt försvar”. Text. 18 december 2025. https://skr.se/civiltforsvarochkrisberedskap/regionensarbetemedkrisberedskapochciviltforsvar.8263.html.

60. *Remissvar avseende kommissionens förordningsförslag om inrättandet av det europeiska försvarsindustriprogrammet (EDIP) 2024 0061 (COD) - SOFF*. EU. 21 mars 2024. https://soff.se/dokument/remissvar-avseende-kommissionens-forordningsforslag-om-inrattandet-av-det-europeiska-forsvarsindustriprogrammet-edip-2024-0061-cod/.

61. ”SECTECH Sweden”. Åtkomstdatum 29 januari 2026. https://www.securityworldmarket.com/sectechexpo/sweden/en.

62. SecurityWorldMarket.com. ”Seriline: NIS2 och CRA kommer rensa bort en hel del mindre aktörer”. Åtkomstdatum 05 januari 2026. https://www.securityworldmarket.com/se/Nyheter/Teman/seriline-om-nis2-och-cra-kommer-rensa-bort-mindre-aktorer.

63. ”SKYDD October 20-22 2026”. 111. Åtkomstdatum 26 januari 2026. https://skydd.net/en/.

64. ”SSG Säkerhetskonferens”. Åtkomstdatum 26 januari 2026. https://www.ssgsolutions.com/sv/aktuellt/konferenser-och-event/ssg-sakerhetskonferens/.

65. ”State of the Union 2025 - European Commission”. 05 september 2025. https://commission.europa.eu/strategy-and-policy/state-union/state-union-2025_en.

66. Sverige. *Säkerhetsskyddslagen: ytterligare kompletteringar*. Regeringskansliet, 2025.

67. ”Säkerhetsdagen”. Åtkomstdatum 26 januari 2026. https://sakerhetsdagen.se/.

68. ”The Cyber Resilience Act - Summary of the Legislative Text | Shaping Europe’s Digital Future”. Åtkomstdatum 05 januari 2026. https://digital-strategy.ec.europa.eu/en/policies/cra-summary.

69. *The state of AI in video surveillance*. Axis Communications AB, u.å. Åtkomstdatum 22 januari 2026. https://www.axis.com/dam/public/permalink/239109/the-state-of-ai-in-video-surveillance--report-en-US_239109.pdf.

70. ”Trygg & Säker - Trygg & Säker”. Åtkomstdatum 29 januari 2026. https://tryggochsaker.se/.

71. Tuohy, Jennifer Pattison. ”Hands-on with Hands-Free Unlocking”. The Verge, 02 februari 2025. https://www.theverge.com/smart-home/603957/uwb-hands-free-unlocking-schlage-aliro-apple-samsung-hands-on.

72. Vd, Anne Haaber-Bernth, och Securitas Technology Sverige. ”Trendrapporten 2026: Från reaktivt skydd till prediktiv trygghet”. 02 december 2025. https://www.securitastechnology.com/sv/blogg/trendrapporten-2026-fran-reaktivt-skydd-till-prediktiv-trygghet.

73. ”Venezuela: Overview of U.S. Sanctions Policy”. Legislation. Åtkomstdatum 22 januari 2026. https://www.congress.gov/crs-product/IF10715.

74. *Verisure Midholding AB Annual Report 2024*. Malmö, u.å. Åtkomstdatum 15 januari 2026. https://www.verisure.com/system/files?file=private_pdf%2F2025-04%2Fverisure-midholding-ab-annual-report-2024.pdf.

75. *Verisure plc Interim Report January - September 2025*. London, u.å. Åtkomstdatum 15 januari 2026. https://www.verisure.com/sites/gv/files/news_files/verisure-q3-2025-interim-report.pdf.

76. ”Verisure Reports Results for Q3 2025”. 26 november 2025. https://www.verisure.com/press-releases/verisure-reports-results-for-q3-2025.

77. Wredenmark, Johannes. ”Fastighetsdagen Göteborg | Fastighetsvärlden”. 27 november 2025. https://www.fastighetsvarlden.se/seminarier/fastighetsdagen-goteborg-2026/.

78. ”Årets stora säkerhetshändelse: SäkerhetsDagen 2026”. Åtkomstdatum 26 januari 2026. https://sakerhetsbranschen.confetti.events/arets-stora-sakerhetshandelse-sakerhetsdagen-2026.

## Om Legacy AB

Legacy AB är ett svenskt konsultbolag specialiserat på verksamhetsutveckling, ledningssystem, certifieringar och säkerhetsprövning. Vi hjälper organisationer, både privata och offentliga, att skapa hållbara, effektiva och trygga processer genom helhetslösningar som sträcker sig från strategi till genomförande.

Med bas i Borås och närvaro över hela Sverige arbetar vi nära våra kunder för att möta framtida utmaningar med professionalism, kvalitet och långsiktigt värdeskapande. Sedvanligt partnerstöd inom revision, ISO-arbete, säkerhetsprövning och utbildningar är kärnan i vår verksamhet, allt för att stärka er konkurrenskraft, regelefterlevnad och operativa robusthet.

*Ditt Legacy Vårt Legacy.*

LEGACY

Legacy AB
Lilla Brogatan 31
503 35 Borås

legacyab.se