Terminologi – Informationssäkerhet

LUNDS UNIVERSITET

Termer och definitioner i detta dokument är gällande inom ramen för universitetets informationssäkerhetsarbete, styrande dokument (ledningssystem) samt annan dokumentation och kommunikation.

Ägare och ansvarig för innehåll och förvaltning: ingegerd.wirehed@rektor.lu.se , CISO

Nya termer och ev. förändringsförslag sänds till informationssakerhet@lu.se

Term	Definition
administratör (IT-system)	Användare som har högre eller andra rättigheter än en vanlig användare, t.ex. systemadministratör, säkerhetsadministratör
användare (IT, information)	Person som utnyttjar information eller en tjänst
användarnamn	Namn som en användare anger för att identifiera sig (logga in) och få tillgång till ett datornät, datorprogram eller en webbsida
assurans	Tilltro till att ett systems eller en produkts säkerhetsfunktioner uppfyller specificerade säkerhetskrav
auktorisation	Fastställande av åtkomsträttigheter för en användare till olika systemresurser
autenticitet	Äkthet
autentisering	Kontroll av användares eller systems identitet för att säkerställa att denne verkligen är den han eller hon utger sig för att vara
back-up	Se säkerhetskopia
behandling (av information)	En åtgärd eller kombination av åtgärder beträffande information oberoende av om de utförs automatiserat eller ej, såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring. Notera att dataskyddslagstiftningen är tillämplig på all *helt eller delvis automatiserad* behandling av personuppgifter samt på *manuell behandling av personuppgifter som ingår i eller är avsedda att ingå i ett register.*
behörighet	Den hierarki av rättigheter i ett datorsystem som är knutna till arbetsuppgifter och befattningar. Behörighet är knuten till identitet, så behörighetskontroll sker efter att användarens identitet har kontrollerats (autentiserats).
botnet	Logiskt nät av datorer som smittats av sabotageprogram som gör det möjligt för utomstående att fjärrstyra dem i syfte att sabotera eller utnyttja dem för egen vinning
brandvägg	Nätverkskomponent som enligt given konfiguration begränsar och övervakar trafik mellan nät
certifikat	Ett certifikat är en elektronisk signatur som används för att identifiera en person, en dator, en organisation eller liknande. Liksom en identitetshandling bevisar ett certifikat att en person är den han utger sig för att vara
certifikatutfärdare	Av flera användare betrodd instans som har till uppgift att skapa och utge användarcertifikat eller andra typer av certifikat
CISO	Chief Information Security Officer. Ref lagstadgad roll, MSBFS 2020:6
cybersäkerhet	En delmängd av informationssäkerhet där cybersäkerhet bara handlar om digital information. Cybersäkerhetsbegreppet är mer strategiskt och fokuserar mer på nationella och internationella nätverk samt hot från externa antagonister. Noteras bör att när man talar om digital information blir det en mix av information och bärare – när man exempelvis klassar information är det inte mediet som klassas utan informationsinnehållet.

cyberrymden	Den del av informationsmiljön som består av de sammanlänkade och av varandra beroende IT-infrastrukturer, som möjliggör kommunikation av data och information. Den inkluderar internet, intranät, telekommunikationssystem, IT-system samt inbyggda processorer och styrenheter. Cyberrymden ses som den gemensamma tekniska infrastrukturen men inte informationen i sig.
DoS attack, dDoS attack	Denial of Service attack (överbelastningsattack, tillgänglighetsattack) är en typ av sabotage där någon överbelastar en server eller router genom att sända enorma mängder felaktiga datapaket så att den till slut kraschar. Distributed Denial of Service Attack är en distribuerad överbelastningsattack där anropen sker från många olika datorer, ofta fjärrstyrda via maskar eller trojaner som infekterat dessa datorer utan ägarnas vetskap.
e-legitimation	Elektronisk legitimationshandling som används för säker identifiering på Internet, t.ex. e-legitimation, elektronisk legitimation, e-leg, eID, BankId.
elektronisk signering, digital signering	Omvandling av t.ex. ett meddelande på ett sätt som endast avsändaren kan utföra och som tillåter mottagaren att kontrollera meddelandets äkthet, innehåll och avsändarens identitet
federerad identitet	En användaridentitet som kan användas inom olika organisationer, eftersom man har enats om hur man ska hantera identiteter över organisationsgränserna. En användare som autentiserat sig hos en organisation kan med automatik bli autentiserad hos en annan organisation som ingår i federationen. Resultatet kan bli en singel sign-on som överskrider organisationsgränserna.
förvaltningsobjekt (även Informationsbärare)	Ett eller flera IT-system som förvaltas gemensamt, omfattande såväl applikation som it-teknik. När det gäller förvaltning av IT-infrastruktur består förvaltningsobjektet oftast enbart av it-teknik. Förvaltningsobjekt, IT-system och system har samma betydelse i denna modell. Ett annat förvaltningsobjekt kan vara en fastighet.
förvaltningsorganisation	En grupp människor som under organiserade former sköter förvaltningen av ett specifikt förvaltningsobjekt
förvaltningsplan	Årligt styrdokument för förvaltningen av ett specifikt förvaltningsobjekt
sekretessbelagd uppgift	Uppgift som omfattas av sekretess enligt OSL, offentlighets- och sekretesslagen
hoax	En lögn, en falsk varning eller uppmaning som ser ut att vara sann.
hot	Något som orsakar eller bidrar till att orsaka att en incident inträffar. Oavsiktligt hot: existerar trots att illasinnad avsikt saknas. Avsiktligt hot: syftar till att skada verksamheten Inre hot: orsakas av individer inom organisationen Yttre hot: har sitt ursprung utanför organisationen
hotbild	Hot som bedöms förekomma mot en viss verksamhet dess tillgångar och resurser
identifiering	Att knyta en person med uppgiven identitetsbeteckning (namn, personnummer eller liknande) till en på förhand registrerad identitet. I de flesta fall förutsätts någon form av identitetskontroll (autentisering).
identitet	Unik beteckning för en viss entitet (person, process, fysisk enhet eller liknande) i ett visst system
information	Innebörd i data Data måste tolkas för att information ska erhållas. Ref Gregory Batesons definition av information som "en skillnad som gör en skillnad". Om mottagarens "bild" av objektet inte har förändrats på något sätt – även en bekräftelse betraktas som förändring – så har mottagaren inte erhållit någon information, bara data eller snarare brus.
informationsbärare	Bär, lagrar eller kommunicerar information. Kan exempelvis vara papper, IT-resurser, människor, system, lagringsmedia, telefoni
informationssäkerhet	Bevarande av konfidentialitet, riktighet och tillgänglighet (och spårbarhet) hos information. Informationssäkerhet är en kombination av administrativ och teknisk säkerhet, där fysisk säkerhet och IT-säkerhet ingår i den tekniska säkerheten

informationssäkerhets-incident	En enskild eller en serie oönskade eller oväntade informationssäkerhetshändelser vilka med stor sannolikhet kan äventyra informationssäkerheten
informationssäkerhets-klassning	Att genom konsekvensanalys värdera sin information utifrån aspekterna konfidentialitet, riktighet och tillgänglighet (samt spårbarhet). Denna klassning ska ske av alt. godkännas av beslutade informationsägare.
informationssäkerhets-krav	De VAD-krav som respektive ägare och förvaltare av informationsbärare ska ta ställning till huruvida man uppfyller för t ex ett enskilt objekt (bärare). Status för kravuppfyllnad/regelefterlevnad ligger till grund för handlingsplan om vad som bör åtgärdas.
informationsägare (se även riskägare)	Avser chef eller enhet som har ansvar för att styra insamling, framtagande, utveckling, underhåll, användning och säkerhet avseende viss/a informationstyp/er i en organisation. Dvs ansvaret för den information som skapas och hanteras inom den egna verksamheten. Ansvaret omfattar bl.a. underhåll av och tillgänglighet hos informationen, dess riktighet samt kontroll av att informationen motsvarar ställda krav. Termen ”ägare” innebär inte att personen har faktisk äganderätt till tillgången. Se även riskägare avseende informationssäkerhetsrisker.
informationsmodell	grafisk beskrivning av de informationsobjekt en viss verksamhet behöver och hur de relaterar till varandra
informationssystem	Applikationer, tjänster eller andra komponenter som hanterar digital information. I begreppet ingår också nätverk och infrastruktur. Ref MSBs definition i MSBFS2020:7
Integritet	Okränkbarhet med förmåga att upprätthålla sitt värde genom skydd mot oönskad förändring, påverkan eller insyn. Kan avse såväl ett tekniskt system (systemintegritet) som en person (personlig integritet)
interoperabilitet	Förmåga och möjlighet hos system, organisationer eller verksamhetsprocesser att fungera tillsammans och kunna kommunicera med varandra genom att överenskomna regler följs
intrång	Oönskad interaktion och aktiviteter mot system – i strid med systemets policy – som kan medföra förändringar, störningar eller skada
IT-systemförvaltare/ IT-systemägare	Verksamhetsspecialist, ansvarar på daglig basis för funktionaliteten och säkerhetsnivå i systemet.
IT-systemförvaltning	De aktiviteter som görs för att hantera ett system i drift, så att det effektivt bidrar till att uppfylla verksamhetens mål.
systemförvaltnings-modell	En systemförvaltningsmodell är ett ramverk som beskriver hur ett förvaltningsarbete kan utföras och organiseras. Modellen ger en normgivande bild av de aktiviteter som utförs för att styra, administrera, utföra förändringsarbeten och stödja användandet av ett förvaltningsobjekt
IT-säkerhet	Säkerhet beträffande IT-system med förmåga att förhindra obehörig åtkomst och obehörig eller oavsiktlig förändring eller störning vid såväl kommunikation som lagring och bearbetning av data. IT-relaterade tekniska säkerhetsåtgärder för att upprätthålla informationssäkerhet
konfidentialitet	Egenskapen att information inte tillgängliggörs eller avslöjas till obehöriga individer, enheter eller processer. Not: Konfidentialitet medför inte automatiskt sekretess, även om det kan finnas en koppling. Därför ska begreppen konfidentialitet och sekretess hållas åtskilda. Sekretess är enbart en benämning på den del av informationen som sorterar under OSL
konsekvens	Resultat av en händelse med negativ inverkan
konsekvensnivå	Avser nivån som gäller utifrån de fyra olika perspektiven. T.ex. 0 är lägst och 3 är högst. 3 används bara i speciella omständigheter. 0 representerar få eller inga konsekvenser.
kontinuitetshantering	Förmågan och beredskapen att hantera avbrott i verksamheten, att minska skador pga. avbrott samt att sörja för att kontinuitet i verksamhetens kritiska processer ligger på en accepterad lägsta nivå.
kryptering	Omvandling av klartext till en, för obehöriga, oläslig kryptotext med hjälp av ett kryptosystem och en krypteringsnyckel.
kryptotext	Text som krypterats. Motsats är klartext.
ledningssystem för Informationssäkerhet (LIS)	System (ej IT-systems) för att fastställa en organisationsprocess för styrning och ledning av informationssäkerhetsarbetet. Det omfattar bl.a. grundprinciper för ledning av arbetet, kunna ställa upp mål samt för att uppnå dessa mål, organisation, resurser samt tekniska respektive administrativa säkerhetsåtgärder. LISet är ett stöd för hur informationssäkerhetsarbetet styrs av ledningen i

	verksamheter. En central del i ett ledningssystem är ledningens uttalade stöd. Översta nivån är den policy som styrelsen antar för informationssäkerhetsarbetet. I styrdokument, riktlinjer och liknande kan sedan den högsta ledningen ge vägledning till chefer och övriga medarbetare. Ref: Standard SS-ISO/IEC 27001:2017 som fastställer krav som en organisation behöver uppfylla när det gäller ledningssystem för informationssäkerhet.
Logg	Insamlad information om de händelser/aktiviteter som utförs i ett system, vilka användare eller systemfunktioner som initierat dessa och vid vilken tidpunkt det skedde.
logiskt gränssnitt	Del av en tjänstebeskrivning som beskriver gränsytor som ska implementeras av producent och konsument i form av anrop, meddelanden och sekvenser. Jämför Tekniskt gränssnitt.
Metadata	Data om data
Lösenord	Kombination av tecken som tillsammans med användarnamn anges för att verifiera användaridentitet
mask	Program som mångfaldigar sig i ett distribuerat system
molntjänst	En teknik där resurser, som till exempel processorkraft, lagring och funktioner, tillhandahålls som tjänster via internet.
oavvislighet	Att en handling inte i efterhand ska kunna förnekas av utföraren. Oförnekbarhet
obehörig åtkomst	Åtkomst av system, resurs eller annat objekt i strid med behörighetsregler
outsourcing	Utkontraktering av någon del av intern verksamhet, process eller IT-relaterad tjänst som tidigare utfördes internt, till en extern leverantör
personuppgifter	All slags information som direkt eller indirekt kan knytas till en fysisk person som är i livet. 1) Ordinära personuppgifter Exempel på ordinära personuppgifter är namn, adress, telefonnummer, e-postadress. Det är personuppgifter som inte ingår i kategori 2 eller 3. 2) Känsliga personuppgifter Vad som utgör känsliga personuppgifter är reglerat i lag. Det är uppgifter om etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening, hälsa, en persons sexualliv eller sexuella läggning, genetiska uppgifter och biometriska uppgifter som används för att entydigt identifiera en person. 3) Extra skyddsvärda personuppgifter Exempel på extra skyddsvärda personuppgifter är personnummer och värderande uppgifter om en person, t ex uppgifter från utvecklingssamtal eller uppgifter om resultat från personlighetstester. Det är personuppgifter som bedömts mer skyddsvärda än ordinära personuppgifter men som inte ingår i kategori 2.
personuppgiftsincident	En säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats
pharming	IP-adressförfalskning, omdirigeringsattack till falsk webbsida
phishing, nätfiske	Attack som via epost söker locka mottagaren att besöka en till synes äkta webbsida (för t.ex. en bank eller kreditkortsföretag) och där uppge inloggningsinformation eller andra känsliga uppgifter
PIN-kod	Personal identification number är ett numeriskt lösenord.
policy	Övergripande avsikt och viljeinriktning formellt uttryckt av ledningen
process	Ett eller flera arbetssteg, som logiskt hänger samman och som medverkar till att ett resultat kan levereras
ransomware, kryptovirus	Skadlig kod som krypterar hela eller delar av innehållet i systemet. Det kan vara viss typ av filer (crypto ransomware) eller att datorn inte kan startas upp (locker ransomware). Angriparen begär en lösensumma för att lämna ut det lösenord som låser upp krypteringen.
riktighet	Egenskapen att skydda exaktheten och fullständigheten gällande tillgångar
risk	En systematisk sammanvägning av förväntad sannolikhet för och konsekvens av att en oönskad händelse inträffar till följd av ett visst hot, kopplat till en definierad verksamhet, en specifik skyddsvärd tillgång och en specifik konsekvensskala. Organisationen identifierar vilka risker som finns (=bruttorisk) och bedömer

	effekten av att risken inträffar (sannolikhet * konsekvens). Därefter Identifiera och utvärdera existerande kontroller/åtgärder för att bedöma kvarvarande risk (=nettorisk). En åtgärdsplan upprättas för att begränsa de nettorisker som man bedömer ligger för högt, trots implementerade kontroller/åtgärder. Efter att brutto- och nettorisker har identifierats behöver verksamheten fatta beslut om vilka aktuella risknivåer som kan accepteras eller om motverkande kontroller behöver stärkas. (Detta moment ingår och beskrivs i sin helhet i metodiken för riskhantering avseende informationssäkerhet).
riskanalys	Process som identifierar hot mot verksamheten och uppskattar storleken hos relaterade risker
riskbedömning	Övergripande process för riskidentifiering, riskanalys och riskutvärdering.
riskhantering	Samordnade aktiviteter för att bedöma (identifiera, analysera och utvärdera) och behandla risker. Vid behandling av risker skapas förebyggande åtgärder för att reducera risken. Två huvudmetoder används. A) Riskreducering genom att skapa en förebyggande åtgärd. Här kan kostnad beräknas, typ anges, ansvarig för åtgärden, koppling till andra risker som denna åtgärd reducerar, tidsram. B) Riskreducering genom att koppla till en kontroll. Kontrollen väljs ur kontroller eller säkerhetsåtgärder. När risken har hanterats finns möjlighet att göra en ny riskbedömning efter att planerade åtgärder är införda. Detta brukar kallas nettorisk och den ursprungliga bedömningen bruttorisk.
riskidentifiering	Process för att upptäcka, kartlägga/känna igen och beskriva risker
riskutvärdering	Process för att jämföra resultaten från riskanalysen med riskkriterierna för att avgöra om risken och/eller dess storlek är acceptabel eller godtagbar
riskägare	Person eller enhet som ansvarar för och har befogenhet att hantera en risk
rootkit	Ett spökprogram som döljer saker för användare och administratörer genom att modifiera systemets funktion
systemrättighet	Användares rätt att utföra olika handlingar på en dator eller i ett nätverk. Rättigheterna gäller sådant som att köra, installera och radera program, hämta, läsa, ändra och lägga till information, ändra inställningar, komma åt, använda och sprida information över nätverket och över internet.
sabotageprogram	En överordnad term för oönskade datorprogram, framför allt virus, maskar, trojaner och hybrider
sekretess, sekretessbelagd uppgift	Ett förbud att röja en uppgift, vare sig det sker muntligen, genom utlämnande av en allmän handling eller på något annat sätt. En sekretessreglerad uppgift för vilken sekretess gäller i ett enskilt fall, enligt OSL, Offentlighets- och Sekretesslagen.
single sign-on (SSO)	En metod för att hantera användare med aspekt på autentisering och auktorisering, så att dessa användare endast behöver logga in en enda gång för att nå de system som är anpassade till tjänsten.
skadlig kod	Otillåten programkod som är till för att ändra, röja, förstöra eller avlyssna ett elektroniskt kommunikationsnät eller funktioner eller uppgifter i ett IT-system
skydd	Effekt av handlingar, rutiner och tekniska arrangemang som syftar till att minska sårbarheten. Motsats till sårbarhet.
skyddsvärde	En verksamhets olika värden (tillgångar) mot vilka det kan riktas risker. Det kan vara information, material, renommé, byggnader, beställningar, nyckelpersoner, beroenden, instrument osv.
sniffer	Anordning eller program som samlar in data som skickas över ett nätverk, en nätlyssnare.
social engineering	Manipulering genom använda olika sociala knep för att skapa förtroende och senare tillgång till känslig eller hemlig information
spam	Massutskick av oönskad, icke beställd e-post, ofta med kommersiellt budskap och utan mottagarens samtycke. Skräppost.
spyware	Spionprogram som körs på en dator utan användarens godkännande, och samlar och vidarebefordrar information till annan part.
spårbarhet	Möjlighet att entydigt kunna härleda utförda aktiviteter i systemet till en identifierad användare vid en viss tidpunkt.

system/IT-system/ informationssystem	Bärare av information. Ärver klassning från informationsinnehållet. Systemperspektivet hjälper till att hitta ägarskap. Fokus är dock på informationen som hanteras i systemet. Uppsättning av applikationer, tjänster, informationsteknologiska tillgångar och andra informationshanteringskomponenter
sårbarhet	Svaghet eller avsaknad av något som skulle kunna förhindra att en incident inträffar, och oönskad konsekvens av en incident. Dessa gäller en tillgång eller grupp av tillgångar, vilken kan utnyttjas av ett eller flera hot.
Säkerhet (eng)	Security - egenskap eller tillstånd som innebär skydd mot risk för oönskad insyn, förlust eller påverkan. Oftast i samband med medvetna försök att utnyttja eventuella svagheter/sårbarheter Safety - egenskap eller tillstånd som innebär skydd mot skada för liv och lem (personsäkerhet)
säkerhetskopia	Kopia av en informationsmängd som skapats för att kunna utnyttjas vid förlust av hela eller delar av den ursprungliga informationsmängden. Se back-up
säkerhetsskydd (Ref: Säkerhetsskyddslagen)	Med säkerhetsskydd avses 1. skydd mot spionerі, sabotage och andra brott som kan hota rikets säkerhet, 2. skydd i andra fall av uppgifter som omfattas av sekretess enligt offentlighets- och sekretesslagen och som rör rikets säkerhet, och 3. skydd mot terroristbrott enligt 2 § lagen om straff för terroristbrott (terrorism), även om brotten inte hotar rikets säkerhet.
tekniskt gränssnitt	Del av en tjänstebeskrivning som beskriver teknikval för olika implementationer i form av exempelvis protokoll och standarder
tillgänglighet	Egenskapen att vara åtkomlig och användbar vid begäran av en behörig enhet, t.ex. användare
tillgänglighetsförlust	Övergång till ett tillstånd hos ett system där det inte i erforderlig utsträckning eller inom önskad tid kan leverera önskade tjänster
tjänst	Paketerad service eller lösning som erbjuds för att tillgodose ett behov
tjänstemeddelande	Den information som förmedlas mellan deltagare i en tjänsteinteraktion
tjänstekatalog	en logisk plats för att söka, hitta, ge åtkomst till, publicera, administrera och lagra beskrivningar av tjänster
trojan	Ett program som utger sig för att vara till nytta eller nöje, men är någon skadlig programkod
tvåfaktors/ flerfaktors-autentisering	Identitetskontroll genom två (eller flera) av faktorerna något man har, något man vet och något man är (t ex kort, lösenord, biometri). Var för sig är kort, kod eller biometri oanvändbar i inloggningssyfte men två tillsammans ger autentisering.
upphandlingskrav	Upphandlingskrav avseende informationssäkerhet utifrån de VAD-krav som fastställts baserat på informationsklassning och kravanalys.
virus	Illasinnad kod som sprider sig genom att lägga en kopia av sig själva inuti andra program, värdprogram, på sådant sätt att koden körs då värdprogrammet körs
åtgärd/säkerhetsåtgärd	Handling, procedur eller tekniskt arrangemang som genom att minska sårbarheten möter identifierat hot. Exempel på typer av säkerhetsåtgärder: Organisatorisk: att man fördelar ansvar, roller och mandat i organisationen så att informationen skyddas mot felaktig hantering (vem gör vad för att undvika att saker hamnar mellan stolarna). Administrativ: att man skapar styrdokument, rutiner eller liknande samt genomför utbildningar som stöd för säker informationshantering. Fysisk: att ha lås, larm, dörrar, fönster och motsvarande som skyddar information och informationssystem mot obehörig fysisk åtkomst. Teknisk: att olika IT-lösningar används för att skydda informationen, till exempel antivirus, behörighetssystem, säkerhetsloggning och säkerhetskopiering.
systemägare	Som systemägare utses normalt den person som är verksamhetsansvarig (dekan, prefekt/motsv.) för att automatiskt få en koppling mellan verksamhetens nytta och

	krav på systemet. Systemägaren har det övergripande ansvaret för visioner och ramar och ska ansvara för att systemet stöttar verksamheten och dess processer på ett ändamålsenligt sätt. Systemägaren ska säkerställa de resursmässiga förutsättningarna och fatta beslut inom systemets budget. Vidare ska systemägaren ansvara för att initiera utvecklingsprojekt. Systemägaren ansvarar för att informationssystemet lever upp till ställda informationssäkerhetskrav. Dessa krav ställs genom utsedd/a informationsägares klassning av den information som systemet används för.
systemförvaltare	Systemförvaltaren arbetar på uppdrag av systemägaren med förvaltning av systemet. Systemförvaltaren arbetar utifrån de mål och aktiviteter som definierats i beslutade planer och inom de ramar som tilldelats för perioden. Systemförvaltaren ska genomföra aktiviteter för att samla in krav och behov från verksamheten och rapportera dessa till systemägaren. Systemförvaltaren leder arbetet i förvaltningsgrupp och referensgrupper.
överföring till tredje land (Ref IMY, GDPR)	Överföring av personuppgifter till tredje land är när personuppgifter blir tillgängliga för någon i ett land utanför EU/EES-området. Detta sker vid universitetet, t ex När ni skickar dokument som innehåller personuppgifter per e-post till någon i ett land utanför EU/EES. När ni anlitar ett personuppgiftbiträde i ett land utanför EU/EES. När ni ger någon utanför EU/EES tillgång, exempelvis läsbehörighet, till personuppgifter som finns lagrade inom EU/EES. När ni lagrar personuppgifter i en molntjänst som är baserad utanför EU/EES. När ni lagrar personuppgifter, till exempel på en server, i ett land utanför EU/EES.