Riktlinjer för hantering av personuppgiftsincident

Dessa riktlinjer omfattar de skyldigheter som den personuppgiftsansvariga har när en personuppgiftsincident inträffar enligt dataskyddsförordningen artikel 33 och 34.

Samlade definitioner

Nedan listas några av de definitioner som beskrivs i dataskyddsförordningen artikel 4 och som kan anses vara aktuella att känna till innan detta dokument läses.

Personuppgifter: varje upplysning som avser en identifierad eller identifierbar fysisk person varvid en identifierbar fysisk person är en person som direkt eller indirekt kan identifieras särskilt med hänvisning till en identifierare som ett namn, ett identifikationsnummer, en lokaliseringsuppgift eller online identifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet.

Behandling: en åtgärd eller kombination av åtgärder beträffande personuppgifter eller uppsättningar av personuppgifter, 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.

Personuppgiftsansvarig: en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter. I detta fall är varje nämnd personuppgiftsansvarig.

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.

Registrerade: Den person vars personuppgifter behandlas

Sammanfattning

För att kunna leva upp till de nya skyldigheter som beskrivs i dataskyddsförordningen artikel 33 och 34 är det viktigt att den personuppgiftsansvarige har rutiner på plats för att upptäcka, rapportera och utreda personuppgiftsincidenter, samt att vid behov göra en extern anmälan till ansvarig tillsynsmyndighet och informera de registrerade som har drabbats.

Den personuppgiftsansvarige ska arbeta proaktivt med säkerhet i samband med behandling av personuppgifter, genom att säkerställa att det finns både lämpliga tekniska och organisatoriska säkerhetsåtgärder implementerade, se även dataskyddsförordningen artikel 32. Detta är ett viktigt arbete för att proaktivt minska antalet potentiella incidenter.

Det är den personuppgiftsansvarige som ansvarar för att anmälan görs, det vill säga den nämnd som bestämmer ändamål och medel för behandlingen.

Riskbedömning och anmälan till Datainspektionen som är tillsynsmyndighet, görs av dataskyddsombudet och ska göras inom 72 timmar från det att incidenten har rapporterats till eller upptäckts av personuppgiftsansvarig.

Under vissa omständigheter är den personuppgiftsansvarige skyldig att informera de personer vars uppgifter berörts av incidenten.

Den personuppgiftsansvarige ska informera om incidentförfarandet så att varje medarbetare vet att de ansvarar för att rapportera risk för, misstanke om eller inträffande av personuppgiftsincident. Rutiner ska finnas i varje verksamhet för hur rapportering görs.

I de fall ett personuppgiftsbiträde har anlitats finns det också en skyldighet för biträdet att uppmärksamma den personuppgiftsansvarige på en personuppgiftsincident så fort den upptäckts. I fall där incidenten upptäcks av den personuppgiftsansvarige och det kan leda till skadestånd eller betalningsansvar för personuppgiftsbiträde ska personuppgiftsansvarig informera personuppgiftsbiträdet om förhållandet och aktivt arbeta tillsammans med personuppgiftsbiträdet för att förhindra och minimera incidenten. Detta bör framgå i de personuppgiftsbiträdesavtal som upprättas.

Alla personuppgiftsincidenter ska dokumenteras och diarieföras av den personuppgiftsansvarige samt rapporteras till dataskyddsombudet. Detta gäller även de incidenter som inte måste anmälas till Datainspektionen.

Allmän översikt

Vad är en incident?

En personuppgiftsincident är en säkerhetshändelse som påverkar sekretessen, integriteten eller tillgängligheten till de personuppgifter som vi behandlar.

En personuppgiftsincident har till exempel inträffat om personuppgifter om en eller flera registrerade personer har, förstörts oavsiktligt, avsiktligt eller olagligt, gått förlorade eller kommit i orätta händer.

En personuppgiftsincident kan innebära risker för människors friheter och rättigheter genom exempelvis att någon förlorar kontrollen över sina uppgifter eller att rättigheterna inskränks och då orsakar skada i form av diskriminering, identitetsstöld, bedrägeri, skadlig ryktesspridning, finansiell förlust eller brott mot sekretess eller tystnadsplikt.

Typer av personuppgiftsincidenter

I sitt yttrande 3/2014 om personuppgiftsbrott förklarade artikel 29-arbetsgruppen att incidenter kan kategoriseras utifrån följande tre välkända informationssäkerhetsprinciper. [1]

- ”Konfidentialitetsbrott” – vid obehörigt eller oavsiktligt röjande av eller åtkomst till personuppgifter.
- ”Integritetsbrott” – vid obehörig eller oavsiktlig ändring av personuppgifter.
- ”Tillgänglighetsbrott” – vid obehörig eller oavsiktlig förlust av åtkomst15 till, eller förstöring av, personuppgifter.

Notera även att en incident, beroende på omständigheterna, på en och samma gång kan röra personuppgifters konfidentialitet, integritet och tillgänglighet, eller varje tänkbar kombination av dessa. Samtidigt som det är relativt lätt att avgöra om det har skett ett konfidentialitets- eller integritetsbrott är det mindre uppenbart huruvida det har skett ett tillgänglighetsbrott. En personuppgiftsincident betraktas alltid som ett tillgänglighetsbrott, även vid permanent förlust eller förstöring av personuppgifter[2]

Bedömning av incident

Inrapporterad incident ska efter riskbedömning klassificeras i en av fyra olika kategorier; obetydlig risk, begränsad risk, mycket allvarlig eller betydande risk. Beroende på bedömd risk utförs sedan ett antal åtgärder.

[1] Se yttrande 3/2014

[2] https://www.datainspektionen.se/globalassets/dokument/riktlinjer-om-personuppgiftsincidenter.pdf

Anmälan av incident till Datainspektionen

Incidenter som bedömts utgöra en begränsad, betydande eller allvarlig risk **ska** anmälas till Datainspektionen utan onödigt dröjsmål, men inte senare än 72 timmar efter upptäckt, om det inte är osannolikt att incidenten medfört en risk för de registrerades fri- och rättigheter.

Information som inte kan lämnas till datainspektionen inom 72 timmar från upptäckt, ska kompletteras i efterhand. Detta ska ske så snart som möjligt.

Hinner man inte göra någon anmälan alls inom 72 timmar ska datainspektionen ändå informeras och skälen till förseningen ska anges.

När ska de registrerade informeras?

Enligt förordningen ska de registrerade direkt och utan onödigt dröjsmål informeras om en personuppgiftsincident sannolikt leder till en hög risk för fysiska personers rättigheter och friheter. Bedömningen ska göras utifrån både allvarligheten av den potentiella eller faktiska påverkan på personer som ett resultat av en personuppgiftsincident kan ha och utifrån sannolikheten för att detta inträffar.

Information till de registrerade i anledning av en personuppgiftsincident behöver inte alltid göras. Den bedömningen får ske från fall till fall.

Följande frågeställningar är en utgångspunkt för bedömningen.

- Hur allvarliga kan konsekvenserna bli?
- Hur sannolikt är det att enskilda personer drabbas?

Om personuppgiftsincidenten är allvarlig är risken högre. Om sannolikheten för konsekvenser är stor är risken också högre.

När risken är hög måste de personer som har drabbats informeras, särskilt om det finns ett behov av att mildra en omedelbar risk för skador. En av huvudorsakerna är att du ska kunna hjälpa dem att vidta åtgärder för att skydda sig mot effekterna av en personuppgiftsincident.

På Datainspektionens hemsida, [3] När ska vi informera de registrerade? finns exempel på olika fall av personuppgiftsincidenter. Exempelsamlingen kommer att uppdateras löpande.

Följande punkter är ett minimikrav i brevet till de registrerade:

- Klar och tydlig beskrivning av personuppgiftsincidenten
- Namn och kontaktuppgifter till dataskyddsombudet
- Beskrivning av de sannolika konsekvenserna av personuppgiftsincidentenBeskrivning av vad vi har gjort, eller tänker göra, för att hantera personuppgiftsincidenten

En av huvudorsakerna till att informera är att hjälpa de registrerade att vidta åtgärder för att skydda sig mot effekterna av en personuppgiftsincident.

När datainspektionen blir informerad om en incident kan myndigheten fatta beslut om att den personuppgiftsansvarige måste informera de registrerade eller att det inte är nödvändigt. Om de registrerade ska informeras kan datainspektionen komma att ge råd om hur detta ska ske.

Hur ska en incident hanteras

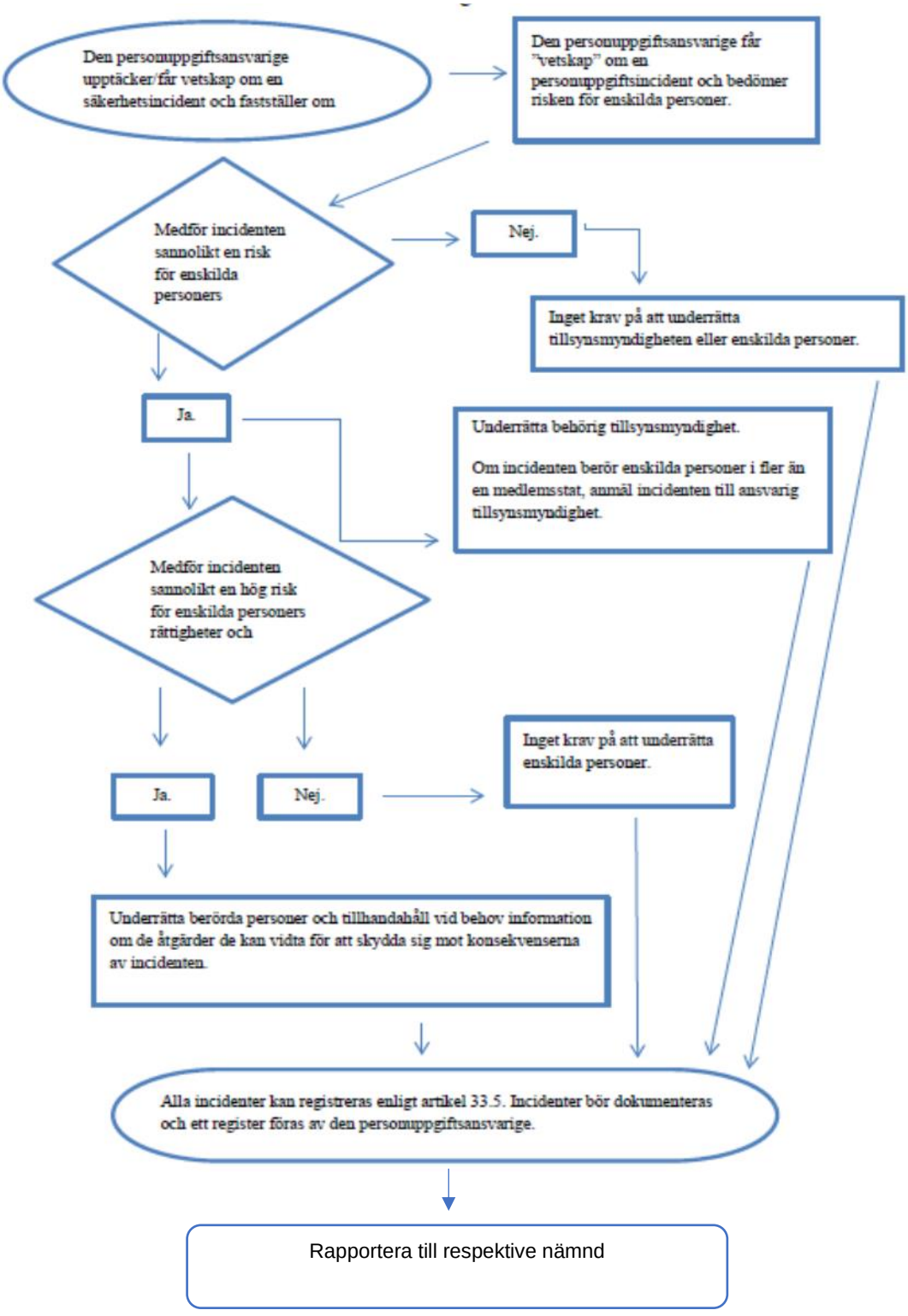
När en misstänkt incident har **identifierats** gäller det att så snabbt som möjligt att **begränsa** skadan, **hantera** omfattningen och **återställa** så långt det är möjligt. Detta görs genom att rapportera incidenten enligt fastställda rutiner.

Riskbedömning ska genomföras tillsammans med dataskyddsombud.

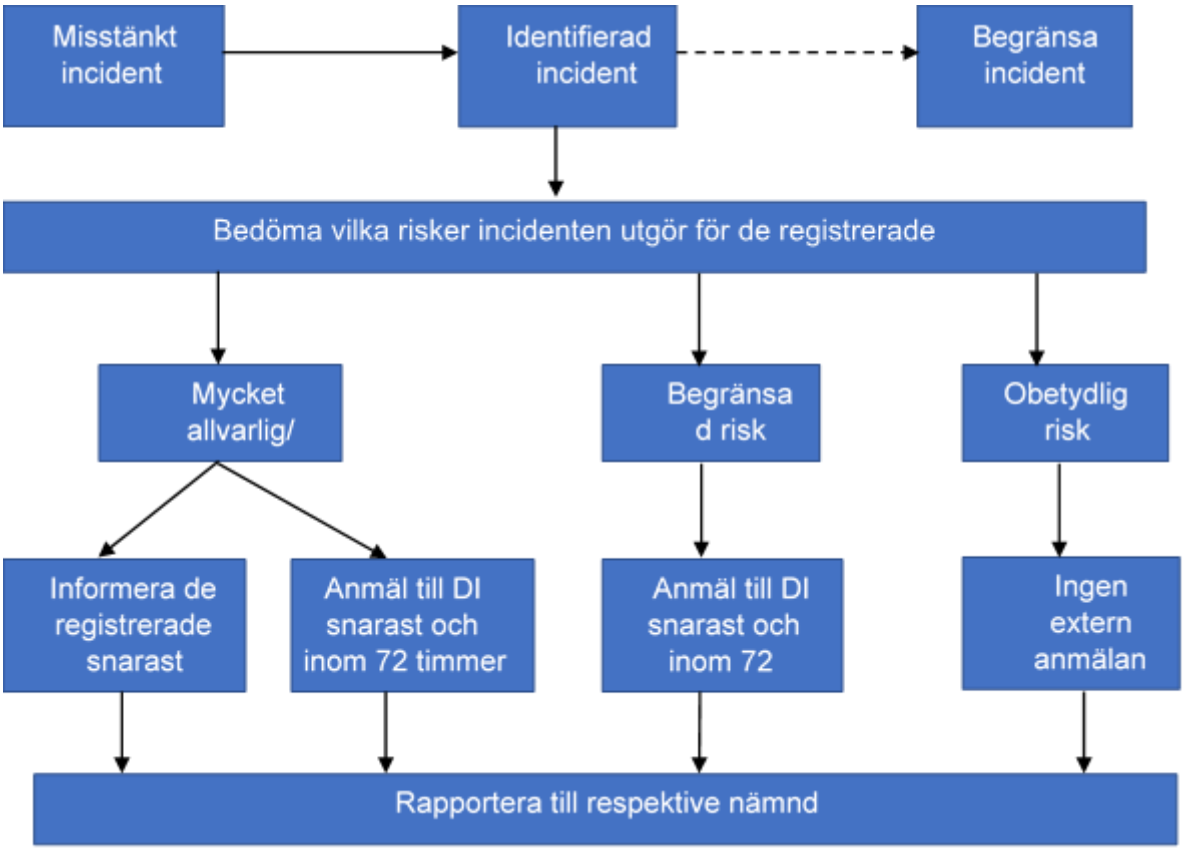
Ibland ska **anmälan** göras till datainspektionen och i vissa fall ska även de drabbade **informeras**. Alla incidenter ska diarieföras, **dokumenteras** och **rapporteras** till dataskyddsombud samt sparas hos av förvaltningen utsedd ansvarig.

[3] https://www.datainspektionen.se/lagar--regler/dataskyddsforordningen/personuppgiftsincident/nar-ska-vi-informera-de-registrerade/

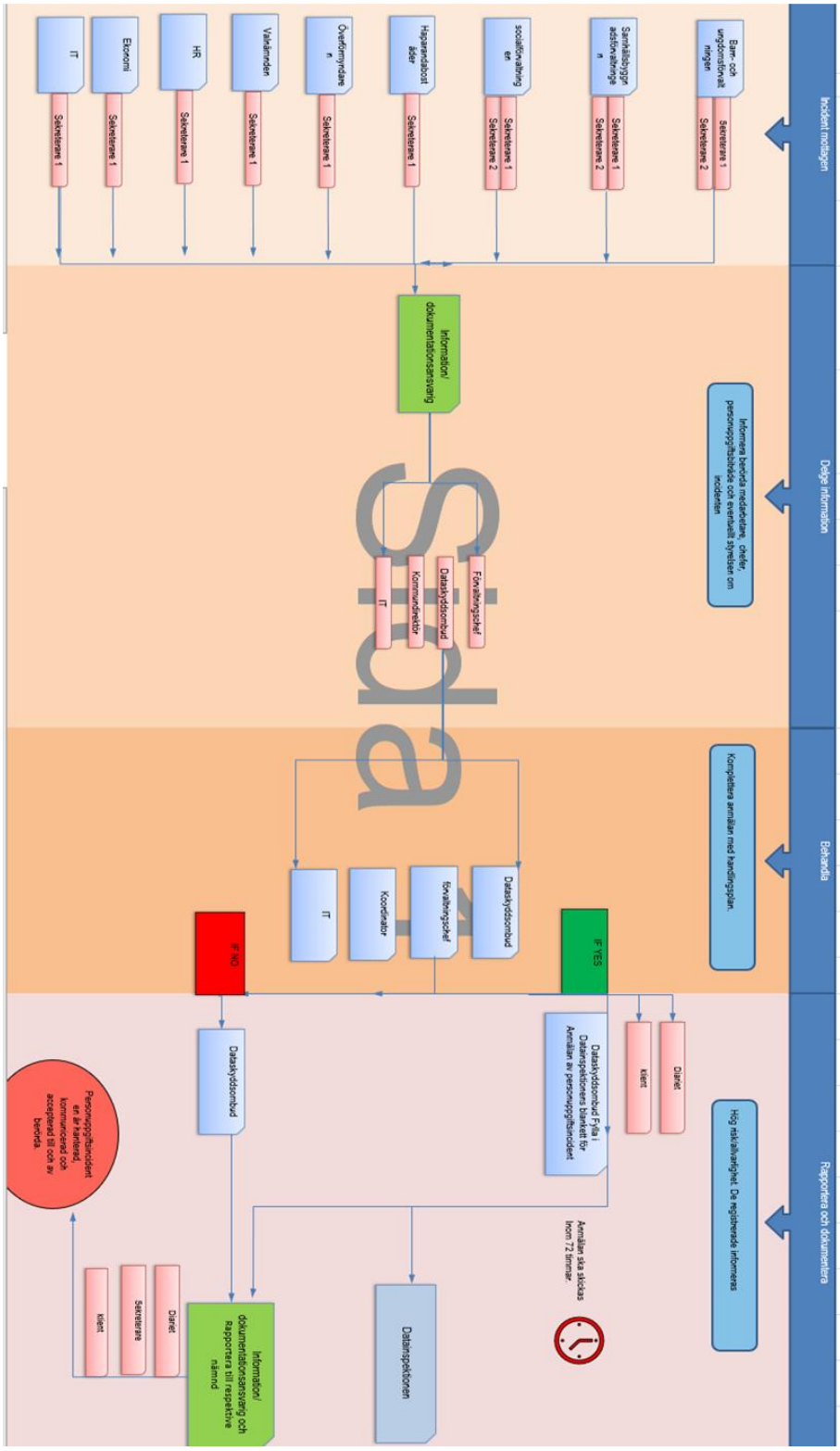
Figur 1: Flödesschema som visar anmälningskrav



Figur 2: Incidenten kan efter riskbedömningen klassificeras i en av fyra olika kategorier, obetydlig, begränsad, betydande eller mycket allvarlig risk.



Figur 3: Hur processhantering kan se ut.



Information till anställda och implementering

Nyanställda

All nyanställd personal ska genomgå en grundläggande utbildning inom dataskydd och GDPR. Utbildningen tar cirka en timme och genomförs av information- och dataskyddshandläggaren

Ansvarig chef bokar in ett informationstillfälle under den nyanställdes introduktion, alternativt någon gång under den anställdes första månad.

Löpande information

Information om incidentrapportering skall ges återkommande till verksamhetens anställda minst en gång per år.

Säkerhet för personuppgifter

Artikel 32-säkerhet i samband med behandlingen

1) Med beaktande av den senaste utvecklingen, genomförandekostnaderna och behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige och personuppgiftsbiträdet vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken, inbegripet, när det är lämpligt
   a) pseudonymisering och kryptering av personuppgifter,
   b) förmågan att fortlöpande säkerställa konfidentialitet, integritet, tillgänglighet och motståndskraft hos behandlingssystemen och -tjänsterna,
   c) förmågan att återställa tillgängligheten och tillgången till personuppgifter i rimlig tid vid en fysisk eller teknisk incident,
   d) ett förfarande för att regelbundet testa, undersöka och utvärdera effektiviteten hos de tekniska och organisatoriska åtgärder som ska säkerställa behandlingens säkerhet.

2) Vid bedömningen av lämplig säkerhetsnivå ska särskild hänsyn tas till de risker som behandling medför, i synnerhet från oavsiktlig eller olaglig förstöring,
3) förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats.
4) Anslutning till en godkänd uppförandekod som avses i artikel 40 eller en godkänd certifieringsmekanism som avses i artikel 42 får användas för att visa att kraven i punkt 1 i den här artikeln följs.
5) Den personuppgiftsansvarige och personuppgiftsbiträdet ska vidta åtgärder för att säkerställa att varje fysisk person som utför arbete under den personuppgiftsansvariges eller personuppgiftsbiträdets överinseende, och som får tillgång till personuppgifter, endast behandlar dessa på instruktion från den personuppgiftsansvarige, om inte unionsrätten eller medlemsstaternas nationella rätt ålägger honom eller henne att göra det.

Artikel 33 - Anmälan av en personuppgiftsincident tillsynsmyndigheten

1) Vid en personuppgiftsincident ska den personuppgiftsansvarige utan onödigt dröjsmål och, om så är möjligt, inte senare än 72 timmar efter att ha fått vetskap om den, anmäla personuppgiftsincidenten till den tillsynsmyndighet som är behörig i enlighet med artikel 55, såvida det inte är osannolikt att personuppgiftsincidenten medför en risk för fysiska personers rättigheter och friheter. Om anmälan till tillsynsmyndigheten inte görs inom 72 timmar ska den åtföljas av en motivering till förseningen.
2) Personuppgiftsbiträdet ska underrätta den personuppgiftsansvarige utan onödigt dröjsmål efter att ha fått vetskap om en personuppgiftsincident.
3) Den anmälan som avses i punkt 1 ska åtminstone.
   a) Om och i den utsträckning det inte är möjligt att tillhandahålla informationen samtidigt, får informationen tillhandahållas i omgångar utan onödigt ytterligare dröjsmål.
   b) beskriva personuppgiftsincidentens art, inbegripet, om så är möjligt, de kategorier av och det ungefärliga antalet registrerade som berörs samt de kategorier av och det ungefärliga antalet personuppgiftsposter som berörs,
   c) förmedla namnet på och kontaktuppgifterna för dataskyddsombudet eller andra kontaktpunkter där mer information kan erhållas,
   d) beskriva de sannolika konsekvenserna av personuppgiftsincidenten, och
   e) beskriva de åtgärder som den personuppgiftsansvarige har vidtagit eller föreslagit för att åtgärda personuppgiftsincidenten, inbegripet, när så är lämpligt, åtgärder för att mildra dess potentiella negativa effekter.
4) Om och i den utsträckning det inte är möjligt att tillhandahålla informationen samtidigt, får informationen tillhandahållas i omgångar utan onödigt ytterligare dröjsmål.
5) Den personuppgiftsansvarige ska dokumentera alla personuppgiftsincidenter, inbegripet omständigheterna kring personuppgiftsincidenten, dess effekter och de korrigerande åtgärder som vidtagits. Dokumentationen ska göra det möjligt för tillsynsmyndigheten att kontrollera efterlevnaden av denna artikel.

Artikel 34-INFORMATION till den registrerade om en personuppgiftsincident

1) Om personuppgiftsincidenten sannolikt leder till en hög risk för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige utan onödigt dröjsmål informera den registrerade om personuppgiftsincidenten.
2) Den information till den registrerade som avses i punkt 1 i denna artikel ska innehålla en tydlig och klar beskrivning av personuppgiftsincidentens art och åtminstone de upplysningar och åtgärder som avses i artikel 33.3 b, c och d.
3) Information till den registrerade i enlighet med punkt 1 krävs inte om något av följande villkor är uppfyllt:
   a. Den personuppgiftsansvarige har genomfört lämpliga tekniska och organisatoriska skyddsåtgärder och dessa åtgärder har tillämpats på de personuppgifter som påverkades av personuppgiftsincidenten, i synnerhet sådana som ska göra uppgifterna oläsbara för alla personer som inte är behöriga att få tillgång till personuppgifterna, såsom kryptering.

b. Den personuppgiftsansvarige har vidtagit ytterligare åtgärder som säkerställer att den höga risk för registrerades rättigheter och friheter som avses i punkt 1 sannolikt inte längre kommer att uppstå.
c. Det skulle inbegripa en oproportionell ansträngning. I så fall ska i stället allmänheten informeras eller en liknande åtgärd vidtas genom vilken de registrerade informeras på ett lika effektivt sätt.

4) Om den personuppgiftsansvarige inte redan har informerat den registrerade om personuppgiftsincidenten får tillsynsmyndigheten, efter att ha bedömt sannolikheten för att personuppgiftsincidenten medför en hög risk, kräva att den personuppgiftsansvarige gör det eller får besluta att något av de villkor som avses i punkt 3 uppfylls.