DIGITALISERINGSSTYRELSEN

Vejledning om hændelsesunderretning i henhold til artikel 19 i eIDAS

2016

Indhold

Ændringslog

1. Ændringslog

Ændringsloggen skal gøre det lettere at overskue de nødvendige ændringer i vejledningen.

Nedenfor fremgår en ændringslog, som gør det muligt for tillidstjenesteudbydere at orientere sig om de løbende ændringer, der vil blive foretaget i vejledningen.

Digitaliseringsstyrelsen har forståelse for, at det kræver ekstra ressourcer for tillidstjenesteudbyderne at følge de løbende ændringer. Ændringerne må dog nødvendigvis foretages, da rammerne – herunder særligt i forhold til Digitaliseringsstyrelsens internationale samarbejde – løbende ændres og tilpasses.

Dato	Ændring
27-06-2016	Vejledning publiceret
08-07-2016	Beskrivelsen af Digitaliseringsstyrelsens underretning til Center for Cybersikkerhed er opdateret og præciseret.

Vejledningens formål og indhold

2. Vejledningens formål og indhold

Nedenfor følger en redegørelse for vejledningens formål og indhold, som skal give læseren et bedre overblik.

Formål
Formålet med dette dokument er at redegøre for tillidstjenesteudbyderes ansvar for at indberette sikkerhedshændelser i forlængelse af eIDAS-forordningens[1] artikel 19 samt at beskrive, hvordan hændelsesunderretning håndteres i praksis. Nedenfor følger en kort opsummering af de enkelte afsnits indhold:

eIDAS' scope og krav om hændelsesunderretning
Her redegøres for forordningens definition af en tillidstjeneste samt hvilke af disse, der falder under forordningens scope. Herefter gennemgås artikel 19s krav om hændelsesunderretning, hvor der også informeres om formålet med hændelsesunderretningen.

Praksis inspireret af ENISAs rammeværk
Digitaliseringsstyrelsen har deltaget i ENISAs ekspertgruppe vedr. artikel 19. Afsnittet giver et indblik i, hvilke krav Digitaliseringsstyrelsen skal løfte i international kontekst, samt hvilket rammeværk styrelsen har ladet sig inspirere af i de praktiske overvejelser.

Vurdering af hændelsers indvirkning
Målet med denne del af vejledningen er at give tillidstjenesteudbyderen indsigt i og værktøjer til at vurdere, hvornår det kan hævdes, at en hændelse har en væsentlig indvirkning og dermed skal indberettes.

Indberetning af hændelser
Her fastlægges de praktiske rammer for hændelsesunderretningen, herunder informationer om, hvordan den foretages, hvilke data der skal indsendes til hvem osv.

[1] Forordningens fulde navn er: "Europa-Parlamentets og rådets forordning (EU) Nr. 910/2014 af 23. juli 2014 om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked og om ophævelse af direktiv 1999/93/EF"

eIDAS' scope og krav om hændelsesunder-retning

3. eIDAS' scope og krav om hændelsesunderretning

Her redegøres for hvilke betingelser, der skal være opfyldt, før en tillidstjeneste er underlagt eIDAS-forordningen, samt hvordan tillidstjenester defineres i forordningen. Endelig oplyses om kravene til hændelsesunderretning.

3.1 Scope

Det fremgår af eIDAS-forordningens artikel 2 stk. 1, at "Denne forordning finder anvendelse på elektroniske identifikationsordninger, der er blevet anmeldt af en medlemsstat, samt på tillidstjenesteudbydere, der er hjemmehørende i Unionen."

Af artikel 2 stk. 2 fremgår dog: "Denne forordning finder ikke anvendelse på levering af tillidstjenester, der udelukkende anvendes i lukkede systemer i henhold til national ret eller aftaler mellem et defineret sæt deltagere."

For yderligere at konkretisere omfanget er det relevant at forholde sig til forordningens definition af en tillidstjeneste. Denne fremgår af artikel 3, 16 og lyder:

»tillidstjeneste«: en elektronisk tjeneste, der normalt udføres mod betaling, og som består af:

a) generering, kontrol og validering af elektroniske signaturer, elektroniske segl eller elektroniske tidsstempler, elektroniske registrerede leveringstjenester og certifikater relateret til disse tjenester, eller
b) generering, kontrol og validering af certifikater for webstedsautentifikation, eller
c) bevaring af elektroniske signaturer, segl eller certifikater relateret til disse tjenester

For yderligere eksemplificering af tillidstjenesteudbyderes processer henvises til ENISAs[2] "Proposal for Article 19 Incident reporting" pkt. 2.2 "Services in scope".

3.2 Artiklens indhold

Kravene til tillidstjenesteudbydere fremgår af stk. 1 og 2 i artikel 19, der for læserens skyld gengives i fuld længde nedenfor:

1. Kvalificerede og ikkekvalificerede tillidstjenesteudbydere skal træffe passende tekniske og organisatoriske foranstaltninger til at styre de sikkerhedsmæssige risici i forbindelse med de tillidstjenester, de udbyder. Under hensyn til den seneste teknologiske udvikling skal disse for-

[2] ENISA er en forkortelse for "European Union Agency for Network and Information Security"

anstaltninger garantere et sikkerhedsniveau, der svarer til risikoens omfang. Tillidstjenesteudbyderne bør navnlig tage skridt til at forhindre og minimere virkningen af sikkerhedsrelaterede hændelser og underrette de berørte parter om de negative virkninger af sådanne hændelser.

2. De kvalificerede og ikkekvalificerede tillidstjenesteudbydere, der konstaterer et brud på sikkerheden eller tab af integritet, som har en væsentlig indvirkning på den udbudte tillidstjeneste eller de berørte personoplysninger, skal hurtigst muligt og under alle omstændigheder inden for 24 timer efter at være blevet opmærksomme på forholdet underrette tilsynsorganet, og eventuelt andre relevante organer som f.eks. det kompetente nationale organ for informationssikkerhed eller databeskyttelsesmyndigheden.

Når det er sandsynligt, at et brud på sikkerheden eller tab af integritet vil krænke den fysiske eller juridiske person, som har modtaget tillidstjenesten, skal tillidstjenesteudbyderen også hurtigst muligt underrette den fysiske eller juridiske person om bruddet på sikkerheden eller tab af integritet.

Hvor det er relevant, og navnlig hvis et brud på sikkerheden eller tab af integritet berører to eller flere medlemsstater, skal det underrettede tilsynsorgan informere tilsynsorganerne i andre berørte medlemsstater og ENISA.

Det underrettede tilsynsorgan skal også informere offentligheden eller kræve, at tillidstjenesteudbyderen gør det, hvis det fastslår, at det er i offentlighedens interesse, at et brud på sikkerheden eller tab af integritet offentliggøres.

3.3 De tre overordnede trin i artikel 19

Artikel 19 opsætter på et overordnet niveau tre krav til såvel kvalificerede som ikkekvalificerede tillidstjenesteudbydere, nemlig at de:

1) Vurderer risici (artikel 19 stk. 1)
2) Foretager passende foranstaltninger for at imødegå risici (artikel 19 stk. 1)
3) Indberetter sikkerhedshændelser til tilsynsorganet og evt. andre relevante organer (artikel 19 stk. 2)

Det følger af "Lov om supplerende bestemmelser til forordning om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked", at Digitaliseringsstyrelsen er tilsynsorgan i Danmark på forordningens område. Hændelser skal dermed indberettes til Digitaliseringsstyrelsen, som også fastlægger de praktiske rammer omkring indberetningen. Bemærk at det også kan være relevant at foretage underretning til Datatilsynet samt andre relevante organer. Digitaliseringsstyrelsen videresender i det omfang, det måtte være relevant, underretninger modtaget i medfør af artikel 19 til Center for Cybersikkerhed som national it-sikkerhedsmyndighed og nationalt kompetencecenter for cybersikkerhed. Det bemærkes i den forbindelse, at fortrolige oplysninger alene må videregives, hvis det har væsentlig betydning for Center for Cybersikkerheds virksomhed.

"Lov om supplerende bestemmelser til forordning om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked" fastsætter i § 6 stk. 2, at manglende overholdelse af sikkerhedskrav og underretningspligten i eIDAS-forordningen straffes med bøde, medmindre strengere straf er forskyldt efter anden lovgivning.

3.4 Formål med indberetning

Det primære formål med underretningspligten er at sikre videndeling. Tilsynsorganer vil videregive de væsentligste af hændelsesunderretningerne til ENISA, Her vil disse kunne danne grundlag for vejledning til såvel den private sektor som tilsynsorganerne og politiske aktører. De vil desuden kunne danne et bedre grundlag for at vurdere eventuelle sikkerhedstiltags effektivitet og danne et mere sammenhængende og realistisk billede af truslen på området, hvilket vil være til gavn for både aktører og borgere.

I eIDAS-forordningen stilles ikke krav om, at tilsynsorganet fører et aktivt tilsyn med ikkekvalificerede tillidstjenesteudbydere. Hændelsesunderretningen giver dog alligevel tilsynsorganet et indblik i sikkerhedsforholdene hos de nationale tillidstjenesteudbydere og er dermed med til at sikre, at tilsynet bliver opmærksomt på, om sikkerhedsforanstaltningerne hos tillidstjenesteudbyderne er tilstrækkelige.

Praksis inspireret af ENI-SAs rammeværk

4. Praksis inspireret af ENISAs rammeværk

Digitaliseringsstyrelsen deltager i en international ekspertgruppe, der arbejder med implementering af artikel 19. National praksis baserer sig på ekspertgruppens vurderinger.

eIDAS-forordningen gælder i samtlige medlemsstater, men der er ikke fastlagt formkrav til håndtering af den her omhandlede hændelsesunderretning.

ENISA har dog etableret en ekspertgruppe med repræsentanter fra medlemsstaterne, hvor Digitaliseringsstyrelsen har deltaget fra dansk side. Gruppen drøfter dels forhold vedr. den praktiske implementering samt den nærmere tolkning af, hvilke kriterier, der skal være opfyldt, før en hændelse har "en væsentlig indvirkning", som det formuleres i artikel 19 stk. 2. Der er enighed om, at nationale forhold kan indgå i denne vurdering.

4.1 Rammeværkets indhold

Det internationale samarbejde har bl.a. resulteret i førnævnte "Proposal for Article 19 Incident reporting". Dokumentet fastlægger bl.a. procedurer for udarbejdelse af de nationale tilsynsorganers, herunder Digitaliseringsstyrelsens årlige rapporter til ENISA, men rådgiver også tilsynsorganerne i forhold til national implementering af de relevante processer forbundet med artikel 19.

Da Digitaliseringsstyrelsen har haft indflydelse på indholdet af "Proposal for Article 19 Incident reporting", er dansk praksis på området i høj grad udført ud fra de råd og retningslinjer, rammeværket indeholder. Digitaliseringsstyrelsen er tøvende med at fastsætte objektive kriterier for, hvornår der skal foretages hændelsesindberetning jf. afsnittet "Vurdering af hændelsers indvirkning".

"Proposal for Article 19 Incident reporting" er primært udarbejdet til medlemsstaternes tilsynsorganer. Det bør dog nævnes, at rammeværket giver et bredere indblik i eksempelvis anden relevant lovgivning, ENISAs anvendelse af indrapporterede hændelser, proces for videregivelse af informationer til andre medlemsstater osv..

Rammeværket og de værktøjer, der knytter sig hertil, kan blive ændrede og opdaterede i lyset af de erfaringer, der gøres.

Vurdering af hændelsers indvirkning

5. Vurdering af hændelsers indvirkning

Forordningens formulering om "en væsentlig indvirkning" kræver yderligere fortolkning. Her redegøres for Digitaliseringsstyrelsens overvejelser og krav. Desuden leveres relevante værktøjer, der understøtter vurderingerne.

Kravene til underretning vedrører hændelser, der "[…]har en væsentlig indvirkning på den udbudte tillidstjeneste eller de berørte personoplysninger[…]". Ansvaret for at foretage de relevante indberetninger er tillidstjenesteudbyderens.

Det er vanskeligt at opstille helt faste rammer for, hvilke hændelser der "har en væsentlig indvirkning", da dette vil basere sig på en helhedsvurdering. Det skal dermed også understreges, at dette dokument samt de dokumenter, der henvises til, ikke kan forstås som fuldstændigt udtømmende i forhold til en definition af, hvilke hændelser tillidstjenesteudbyderen bør underrette tilsynsorganet om.

Af formuleringen "en væsentlig indvirkning" kan dog udledes, at der er en bagatelgrænse, som betyder, at hændelser, der enten ikke har indvirkning, eller har en ubetydelig indvirkning, ikke skal indrapporteres. Eksempelvis vil mislykkede angreb mod tillidstjenesten ikke skulle indberettes, da de netop ikke vil have indvirkning på denne. Dog opfordres der til, at mislykkede angreb mod tillidstjenesten indberettes til CFCS, såfremt de ville have haft en væsentlig indvirkning, hvis de var blevet gennemført.[3]

5.1 Niveauopdeling af hændelser

ENISA har i "Proposal for Article 19 Incident reporting" pkt. 3.2.1 oplistet 5 niveauer for hændelsers indvirkning. De beskrives som følger:

1. Ingen indvirkning
2. Ubetydelig indvirkning
3. Betydelig indvirkning
4. Voldsom indvirkning
5. Katastrofal indvirkning

Digitaliseringsstyrelsen ønsker at anvende samme kriterier i forhold til hændelsesindberetninger vedrørende hændelser, hvilket betyder, at hændelser på niveau 1 og 2 ikke skal indberettes. Dette følger også logisk af, at kriteriet for indberetning er, at hændelsen skal have en væsentlig indvirkning.

[3] Center for Cybersikkerhed kan i disse tilfælde kontaktes på:
email: underretning@cfcs.dk/vagttelefonen: 60 93 48 27

Fra niveau 3 og opefter er der tale om hændelser, der har en sådan karakter, at de kan vurderes at have en væsentlig indvirkning på den udbudte tillidstjeneste eller de berørte personoplysninger. Der henvises til "Proposal for Article 19 Incident reporting" pkt. 3.2.1 for en mere fuldstændig og eksemplificeret gennemgang af de 5 niveauer.

De fem niveauer kan ses som en første tilgang til problematikken om hvilke hændelser, der skal indberettes.

Mere detaljeret og omfattende fremstilles forholdene i den model for impact assessment, som ENISA har udarbejdet. Nedenfor findes en overordnet fremstilling af modellen, der viser, hvordan man vurderer en hændelses indvirkning for de enkelte tjenester. Digitaliseringsstyrelsen har slettet henvisningerne til, om tjenesterne er kvalificerede eller ej. Skemaet viser, hvordan man vurderer en hændelses indvirkning, hvis en af ydelserne er kompromitteret i forhold til tilgængelighed, integritet og fortrolighed.

	Tilgængelighed	**Integritet**	**Fortrolighed**
Udstedelse af certifikater	Middel	Høj	Høj
Tidsstempler	Medium	Høj	Lav
Validering af certifikater	Høj	Høj	Lav
Generering og validering af elektroniske signaturer og segl	Medium	Høj	Høj
Elektroniske registrerede leveringstjenester	Medium	Høj	Lav
Bevaring af elektroniske signaturer og segl	Medium	Høj	Lav

Vurderingerne er yderligere udspecificeret i afsnit 6. Her har ENISA systematisk gennemgået hvilke aktiver, der er forbundet med at drive tillidstjenester ud fra ovenfor viste logik.

5.2 Integritet og fortrolighed

På baggrund af ovenstående kan det konkluderes, at samtlige faktiske kompromitteringer af integritet må betragtes som væsentlige og derfor skal medføre, at der foretages underretning. For samtlige områder, hvor fortrolighed er markeret som "medium" eller "high" i afsnit 6, skal der desuden foretages underretning.

5.3 Grænseværdier for tilgængelighed

Nedenfor oplistes de absolutte grænseværdier for hændelser, der vedrører tilgængelighed. Har hændelsen betydelig indvirkning, skal der foretages underretning, uanset om de objektive værdier for hændelsen er lavere end de absolutte grænseværdier.

30 % af brugerne er forhindrede i at bruge tjenesten i en periode af 12 timers varighed.

6. ENISAS konsekvensvurdering

Nedenfor findes ENISAs vurdering af alvorsgraden af hændelser, der vedrører tilgængelighed, integritet eller fortrolighed. Man har oplistet de aktiver (software og hardware), der er forbundet med at drive de tillidstjenester, der er omfattet af forordningen. Det bemærkes, at Digitaliseringsstyrelsen ikke skelner mellem kvalificerede og ikke kvalificerede tjenester i denne kontekst. Oplistningen er en vurdering af, hvornår hændelser har en sådan karakter, at tilsynsorganet skal orientere ENISA om hændelsen. Det vil sige, at listen kan betragtes som absolutte minimumskrav.

SERVICES	**ASSETS**			**Availability**	**Integrity**	**Confidentiality**
Issuance of qualified certificates	CA Platform	Hardware	CA root(s) server(s)	High	NA	NA
Issuance of qualified certificates			HSM CA root(s)	High	NA	NA
Issuance and validation of qualified certificates			SubCA(s) (issuing CA) server	High	NA	NA
Issuance and validation of qualified certificates			Other CA equipment	High	NA	NA
Issuance and validation of qualified certificates			HSM subCA(s)	High	NA	NA
Issuance of qualified certificates		Software	CA root(s) certificate(s)	Medium	High	Low

Issuance of qualified certificates			HSM CA root(s) storing CA root private key	High	High	High
Issuance and validation of qualified certificates			subCA(s) certificate	Medium	High	Low
Issuance and validation of qualified certificates			HSM storing subCA(s) private key(s) and certificate(s)	High	High	High
Issuance and validation of qualified certificates			CA software	Medium	High	Medium
Issuance and validation of qualified certificates, generation, validation and preservation of electronic signatures/seals			CARL	High	High	Low
Validation of qualified certificates, electronic registered delivery, generation, validation and preservation of electronic signatures/seals			CRL	High	High	Low
Issuance of qualified certificates	RA platform	Hardware	RA equipment	High	NA	NA
Issuance of qualified certificates			RA operator devices	Medium	NA	NA
Issuance of qualified certificates		Software	RA software	Medium	High	Medium
Issuance of quali-			RA operator	Medium	High	Low

fied certificates			certificate			
Issuance and validation of qualified certificates, electronic registered delivery, generation, validation and preservation of electronic signatures/seals	VA platform	Hardware	VA server(s)	High	NA	NA
Issuance and validation of qualified certificates, electronic registered delivery, generation, validation and preservation of electronic signatures/seals			HSM(s) for VA(s)	High	NA	NA
Issuance and validation of qualified certificates, electronic registered delivery, generation, validation and preservation of electronic signatures/seals		Software	VA software	Medium	High	Medium
Issuance and validation of qualified certificates, electronic registered delivery, generation, validation and preservation of electronic signatures/seals			VA certificate(s)	Medium	High	Low
Issuance and validation of qualified certificates, electronic registered delivery, generation, validation and preservation of electronic			HSM storing VA(s) private key(s) and certificate(s)	High	High	High

signatures/seals						
Electronic time stamp, electronic registered delivery, generation, validation and preservation of electronic signatures/seals	TSA platform	Hardware	TSA server(s)	High	NA	NA
Electronic time stamp, electronic registered delivery, generation, validation and preservation of electronic signatures/seals			HSM(s) for TSA(s)	High	NA	NA
Electronic time stamp, electronic registered delivery, generation, validation and preservation of electronic signatures/seals		Software	TSA software	Medium	High	Medium
Electronic time stamp, electronic registered delivery, generation, validation and preservation of electronic signatures/seals			TSA certificate(s)	Medium	High	Low
Electronic time stamp, electronic registered delivery, generation, validation and preservation of electronic signatures/seals			HSM storing TSA(s) private key(s) and certificate(s)	High	High	High
Issuance and validation of qualified certificates, Electronic time stamp, electronic registered	Archive		Documentation	Medium	High	High

delivery, generation, validation and preservation of electronic signatures/seals						
Issuance and validation of qualified certificates, Electronic time stamp, electronic registered delivery, generation, validation and preservation of electronic signatures/seals	Network platform		Communication lines, firewalls, etc.	High	High	High
Issuance of qualified certificates, generation and validation of electronic signatures/seals	Subject device	Hardware	Smartcard, USB token, FIDO, mobile, browser, …	High	NA	NA
Issuance of qualified certificates, generation and validation of electronic signatures/seals			Subject certificate	Medium	High	Medium
Issuance of qualified certificates, generation and validation of electronic signatures/seals			Subject keys	High	High	High
Issuance of qualified certificates, generation and validation of electronic signatures/seals	Remote subject device		HSM or webserver storing keys and certificates	High	High	High
generation and validation of electronic signa-	Generation and validation of signatures/seals		Signing software	Medium	High	Medium

tures/seals	platform					
generation and validation of electronic signatures/seals			Signing tool certificate(s)	Medium	High	NA
generation and validation of electronic signatures/seals	Subject device for local signing		Smartcard reader, USB port, …	Medium	High	High
generation and validation of electronic signatures/seals	Documentation uploaded		Documents signed remotely	Medium	High	High
Preservation of electronic signatures/seals	Preservation of signatures/seals platform		Preservation software	Medium	High	Medium
Preservation of electronic signatures/seals			Preservation tool certificate(s)	Medium	High	NA
Preservation of electronic signatures/seals	Documentation uploaded		Documents preserved remotely	Medium	High	Medium
electronic registered delivery	Registered delivery platform		Registered delivery software	Medium	High	Medium

Indberetning af hændelser

7. Indberetning af hændelser

Nedenfor fremgår, hvordan hændelsesunderretningen foretages i praksis.

Ifølge artikel 19 stk. 2 skal tillidstjenesteudbyderen "[…] hurtigst muligt og under alle omstændigheder inden for 24 timer efter at være blevet opmærksomme på forholdet underrette tilsynsorganet, og eventuelt andre relevante organer som f.eks. det kompetente nationale organ for informationssikkerhed eller databeskyttelsesmyndigheden."

7.1 Ikke et kriseberedskab

Den hændelsesunderretning, der foretages i henhold til eIDAS-forordningens artikel 19, har ikke karakter af krisehåndtering men sker primært med henblik på videndeling, der i højere grad tjener mere analytiske formål.

Tillidstjenesteudbyderen må dermed ikke undlade at foretage de sædvanlige skridt i forbindelse med en eventuel krisehåndtering, blot fordi der foretages underretning til tilsynsorganet i Digitaliseringsstyrelsen.

7.2 De relevante organer i dansk kontekst

Som det fremgår af artikel 19 stk. 2, er det tillidstjenesteudbyderen, der foretager indberetning ikke blot til tilsynsorganet men også til eventuelt andre relevante myndigheder. Digitaliseringsstyrelsen har dog indgået en aftale med Center for Cybersikkerhed om, at tilsynet i relevant omfang videresender indberetninger til centeret, hvorfor tillidstjenesteudbyderen i den henseende ikke behøver at gøre sig overvejelser

Tillidstjenesteudbyderen bør stadig forholde sig til, om Datatilsynet bør underrettes.

Det er ligeledes tillidstjenesten, der underretter eventuelle fysiske eller juridiske personer, hvis integritet kan være krænket i forbindelse med, at de har modtaget tillidstjenesten.

Det er tilsynsorganet, der vurderer, om det er relevant at informere andre berørte medlemsstater og ENISA. Dette baserer sig i høj grad på en vurdering af, om flere medlemsstater er berørt af hændelsen.

Orientering af offentligheden foretages udelukkende, hvis det vurderes, at hændelsen har en sådan karakter, at det er relevant. Tilsynsorganet kan foretage underretningen eller kræve, at tillidstjenesteudbyderen gør det.

7.3 Hændelsesunderretning i praksis

Tillidstjenesteudbyderen foretager indberetning til tilsynet ved at udfylde de hertil udarbejdede formularer, eller indsende anden rapportering, der som minimum indeholder de metadata, der fremgår nedenfor. Underretning kan foretages på dansk eller engelsk.

Der er udarbejdet to formularer til formålet, nemlig en foreløbig og en endelig. Det er dermed muligt at fremsende en foreløbig rapport i løbet af de første 24 timer efter hændelsen for efterfølgende at fremsende en endelig, når der er opnået større kendskab til hændelsens årsag, omfang osv. Er tillidstjeneudbyderen i udgangspunktet i besiddelse af samtlige relevante oplysninger, anvendes den endelige rapport.

Hvis tillidstjenesteudbyderen ikke anvender de førnævnte skabeloner, skal indberetningen som minimum indeholde følgende data:

Foreløbig rapport:

- Tillidstjenesteudbyderens navn
- Tillidstjenesteudbyderens kontaktoplysninger
- Dato og tidspunkt, hvor man blev opmærksom på hændelsen (eller hændelsestidspunktet hvis kendt)
- Udbyderens navn
- Tillidstjeneste(r), der er ramt: beskrivelse af tjenesten/tjenesterne
- Personoplysninger der er eller kan være berørt: beskrivelse af hvilken type persondata, der er tale om.
- Kort beskrivelse af sikkerhedshændelsen
- Iværksatte eller planlagte initiativer
- Hændelsens grænseoverskridende konsekvens
- Er databeskyttelsesmyndigheden underrettet?
- Er der foretaget underretning til fysiske eller juridiske personer (hvis relevant)?
- Er andre organer underrettet og i givet fald hvilke?

Endelig rapport:

- Tillidstjenesteudbyderens navn
- Tillidstjenesteudbyderens kontaktoplysninger
- Dato og tidspunkt, hvor man blev opmærksom på hændelsen
- Dato og tidspunkt for hændelsen
- Udbyderens navn
- Tillidstjeneste(r), der er ramt: beskrivelse af tjenesten/tjenesterne
- Sikkerhedshændelsens område: fortrolighed, tilgængelighed og/eller integritet

- Personoplysninger (om nogen) der er berørt: beskrivelse af hvilken type person-data, der er tale om
- Antal brugere, der er påvirkede
- Hændelsens varighed
- Root cause: (eksempelvis menneskelig fejl, systemfejl, cyberangreb, naturkatastrofer etc.)
- Detaljeret beskrivelse af sikkerhedshændelsens årsag
- Detaljeret beskrivelse af berørte aktiver
- Samlet beskrivelse af sikkerhedshændelsen: Fx hvilke systemer er påvirket, hvordan blev man opmærksom på hændelsen, er der svagheder i tredjeparts-software og lign.
- Er databeskyttelsesmyndigheden underrettet?
- Er der foretaget underretning til fysiske eller juridiske personer (hvis relevant)?
- Er andre organer underrettet og i givet fald hvilke?

Rapporterne sendes til tilsyn_eidas@digst.dk

Tillidstjenesteudbyderen har mulighed for at sende krypteret til postkassen. Certifikat til postkassen kan hentes her.

[Indsæt tekst her eller slet (max. 800 anslag)]

digst.dk