DATATILSYNET

Oplysningsskema vedrørende kryptering af e-mails

Datatilsynet skal informere om, at Datatilsynet er dataansvarlig for behandlingen af de personoplysninger, der indsamles i forbindelse med tilsynsbesøget, herunder i dette oplysningsskema. Oplysningerne vil blive brugt i forbindelse med tilsynsbesøget og vil indgå i Datatilsynets tilsyn med behandling af oplysninger, der er omfattet af databeskyttelsesforordningen og databeskyttelsesloven. Oplysningerne vil endvidere kunne anvendes til statistik. Oplysninger indsamlet i oplysningsskemaet kan tænkes videregivet i forbindelse med anmodninger om aktindsigt efter offentligheds- og/eller forvaltningsloven.

Hvis der er uklarheder omkring spørgsmålene, kan Datatilsynet kontaktes for en afklaring.

Spørgsmål 1

Sender XXX følsomme og/eller fortrolige personoplysninger via e-mail over åbne netværk?

Et åbent netværk er et netværk, som den dataansvarlige ikke har fuld kontrol over, fx internettet.

Fortrolige oplysninger kan f.eks. være oplysninger om strafbare forhold og personnummer. Følsomme oplysninger er oplysninger om race eller etnisk oprindelse, politisk, religiøs eller filosofisk overbevisning eller fagforeningsmæssigt tilhørsforhold samt behandling af genetiske data, biometriske data med det formål entydigt at identificere en fysisk person, helbredsoplysninger eller oplysninger om en persons seksuelle forhold eller seksuelle orientering.[1]

Spørgsmål 2

Hvis spørgsmål 1 besvares bekræftende:

Redegør for hvilke typer modtagere (fx klienter, andre virksomheder eller myndigheder) XXX sender fortrolige og/eller følsomme personoplysninger til via e-mail over åbne netværk.

Spørgsmål 3

Hvis spørgsmål 1 besvares bekræftende:

Redegør for i hvilke sammenhænge XXX sender fortrolige og/eller følsomme personoplysninger via e-mail over åbne netværk.

Spørgsmål 4

Hvis spørgsmål 1 besvares bekræftende:

Har XXX siden 1. januar 2019 anvendt kryptering i alle tilfælde, når følsomme og/eller fortrolige personoplysninger er blevet sendt via e-mail over åbne netværk.

Spørgsmål 5

Hvis XXX anvender kryptering besvares følgende:

Redegør for hvem i organisationen der kan sende krypterede e-mails, herunder kategorier af ansatte, med angivelse af hvor mange der er i hver kategori.

Spørgsmål 6

Hvis XXX anvender kryptering besvares følgende:

Redegør for hvilke afsenderadresser, der kan afsende krypterede e-mails, herunder om de under spørgsmål 5 nævnte ansatte kan sende krypteret fra personlige adresser, eller om der afsendes fra enkelte "hovedadresser".

[1] XXX kan læse mere om de forskellige typer af personoplysninger her: https://www.datatilsynet.dk/generelt-om-databeskyttelse/hvad-er-personoplysninger/

Spørgsmål 7

Hvis XXX anvender kryptering besvares følgende:

Redegør for hvilken metode der anvendes til kryptering, når fortrolige og/eller følsomme personoplysninger sendes via e-mail over åbne netværk.

Metoder kan fx være kryptering på transportlaget via TLS, end-to-end kryptering via NemID, PGP, S/MIME, eller kryptering af vedhæftede filer, osv.

Spørgsmål 8

Hvis XXX anvender kryptering besvares følgende:

Redegør for:

a) Baggrunden for den valgte krypteringsform.
b) Hvornår krypteringen benyttes.
c) Hvilket software – herunder biblioteker (konkrete implementeringer; 'libraries') – der benyttes.
d) Hvilke versioner der anvendes/understøttes (fx om der understøttes TLS 1.1 eller TLS 1.2).
e) Hvilke krypteringsalgoritmer/cipher suites, der benyttes.

Spørgsmål 9

Hvis XXX anvender kryptering besvares følgende:

Redegør for:

a) Hvordan løsningen er blevet integreret i XXXs system(er) til afsendelse af e-mail.
b) Hvordan løsningen anvendes.
c) Hvilke tekniske foranstaltninger der er truffet i forbindelse med anvendelsen af løsningen (fx om der bliver skannet efter personnumre, om der anvendes dialogbokse, osv.).
d) Hvilke organisatoriske foranstaltninger der er truffet for, at løsningen bliver benyttet korrekt (fx uddannelse af personale osv.)

Spørgsmål 10

Hvis XXX anvender kryptering besvares følgende:

Redegør for hvordan mailserveren er opsat i forhold til kryptering, herunder

a) Hvilket operativ system der kører på mailserveren.
b) Hvilken mailserver software der anvendes.
c) Hvilket eventuelt tredjepartssoftware der anvendes til fremsendelse af e-mail.

For alle angivne systemer og software skal versionsnummer angives.

Spørgsmål 11

Hvis XXX ikke anvender kryptering til at sende fortrolige og/eller følsomme personoplysninger via e-mail over åbne netværk bedes XXX redegøre for:

a) Hvad baggrunden herfor er.
b) Hvilke andre tekniske eller organisatoriske sikkerhedsforanstaltninger XXX – i henhold til databeskyttelsesforordningens artikel 32 – har truffet for at sikre et sikkerhedsniveau, der passer til risiciene for de registreredes rettigheder.

Spørgsmål 12

Hvis XXX anvender databehandlere til fremsendelse af e-mails, bedes XXX indsende en kopi af databehandleraftalen indgået med den pågældende databehandler i en version, der er gældende pr. 1. januar 2019.

Hvis der er foretaget ændringer i databehandleraftalen mellem den 1. januar 2019 og den 28. februar 2019, bedes XXX ligeledes indsende en kopi af denne aftale med datering.

Spørgsmål 13

XXX bedes fremsende følgende bilag:

a) En kopi af den risikovurdering XXX – i henhold til databeskyttelsesforordningens artikel 32, stk. 1 – har foretaget i forhold til afsendelse af fortrolige og/eller følsomme personoplysninger via e-mail over åbne netværk.
b) Kopier af samtlige relevante konfigurationsfiler der dækker perioden 1. januar 2019 til den 28. februar 2019.
c) Kopier af samtlige relevante public keys og certifikater der dækker perioden 1. januar 2019 til den 28. februar 2019.
d) Øvrige bilag, som XXX vurderer relevante.

Sammen med bilagene bedes fremsendt en kortfattet oversigt over de enkelte bilag.

Datatilsynet skal gøre opmærksom på, at alt materiale skal være **dateret og tilsendt i anonymiseret form**.