Ilinniartitaanermut, Kultureqarnermut, Ilisimatusarnermut,
Ilageeqarnermullu Naalakkersuisoq
Naalakkersuisoq for Uddannelse, Kultur, Forskning og Kirke

NAALAKKERSUISUT
GOVERNMENT OF GREENLAND

Indgået

Ineqi Kielsen
Medlem af Inatsisartut, Siumut

20 FEB. 2017

NAMMINERSORLUTIK OQARTUSSAT
GRØNLANDS SELVSTYRE
INATSISARTUT ALLATTOQARFIAT
BUREAU FOR INATSISARTUT
BOX 1060 - 3900 NUUK

Vedr. § 37 spørgsmål 72, om personoplysninger

Brevdato:17/2-2017

Sags nr.
2017 - 3294
Akt. nr. 4536165

Postboks 1029
3900 Nuuk
Tlf: +299 34 50 00
Fax:+299 32 20 73
Email: ikiin@nanoq.gl
www.nanoq.gl

Kære Ineqi Kielsen,

Tak for dit spørgsmål vedr. beskyttelse af personoplysninger, som jeg vil besvare herunder.

Spørgsmål: *Har Naalakkersuisut procedurer/regler for dokumenter, hvor det er nødvendigt, at der skal træffes sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning?*

Svar: Naalakkersuisut har indført F2 som Selvstyrets elektroniske sags- og dokumentbehandlingssystem. F2 er opsat på en måde, som sikrer, at Selvstyret overholder kravene fra sagsbehandlingsloven, arkivloven og senest også persondata-anordningen.

Ansvaret for, at de fornødne tekniske sikkerhedsforanstaltninger er tilstrækkelige, er placeret hos Digitaliseringsstyrelsen, som dermed har fået rollen som databehandler i Persondata-anordnings terminologi.

Digitaliseringsstyrelsen udarbejder instrukser og procedurer, der sikrer, at de tekniske sikkerhedsforanstaltninger overholdes. Der må ikke foretages ændringer i Selvstyrets IT-netværk eller oprettes nye servere uden godkendelse fra Digitaliseringsstyrelsens driftsafdeling. På den måde undgår man, at der foretages ændringer, der kan udgøre en sikkerhedsmæssig risiko for andre IT-systemer.

Tildeling af adgang til et IT-system administreres af Digitaliseringsstyrelsen. Alle adgange til Selvstyrets IT-systemer styres af Selvstyrets Active Directory (AD).
Der er procedurer for ansættelse og ophør af ansættelsesforhold. Digitale formularer til disse processer findes på intranettet nanuaraq.gl.

Som en særlig sikkerhedsprocedure sletter Digitaliseringsstyrelsen alle adgange til IT-systemer, såfremt de har været inaktive i 13 måneder. Adgang til IT-leverandører gives kun tidsbegrænset til enkeltpersoner. Derudover logges adgangen til alle IT-systemer, så det efterfølgende er muligt at holde opsyn med, hvem der har haft adgang og til hvad.

Beskyttelse af personoplysninger handler også om menneskelig adfærd, og det er den dataansvarlige enheds ansvar, at medarbejderne er indforstået med dette.

Enhederne støttes teknisk af, at nye elektroniske dokumenter, som modtages i F2, altid modtages på sikkerhedsniveauet "Involveret". Det betyder, at det kun er den modtagende medarbejder, der har adgang til dokumentet. Herefter skal medarbejderen lægge det modtagne dokument på den rigtige sag og ændre adgangsrettighederne til "Enheden".

Sikkerhedsgrupperne bestemmer, hvilke personer som kan få adgang til dokumentet. En medarbejder kan på en sag eller et dokument selv ændre indstillingerne, og således give en kollega adgang til sagen eller dokumentet, hvis der er behov for det. Ændringer i forhold til den tekniske standardprocedure hører under den organisatoriske sikkerhed og er dermed den dataansvarlige enheds ansvar.

Det er et krav for alle IT-systemer, at sikkerhedsbehovet fastsættes. Jo højere sikkerhedsvurdering er, jo højere er omkostningerne for den tekniske drift og vedligeholdelse. Da F2 er et fælles IT-system for alle enheder i Selvstyret, er der i dette tilfælde tale om en klassificering på højeste niveau.

For at tydeliggøre ansvarsforholdene mellem Digitaliseringsstyrelsen og de enkelte enheder er Digitaliseringsstyrelsen i gang med at udarbejde en standard databehandleraftale, der præciserer enhedernes ansvar som dataansvarlige og Digitaliseringsstyrelsen ansvar som databehandler.

Det kan ikke anbefales, at enhederne opbevarer elektroniske dokumenter udenfor Selvstyrets IT-systemer. Det er sandt, at Selvstyrets IT-systemer kan udsættes for cyberangreb, men Digitaliseringsstyrelsen, Selvstyrets drifts- og netværksleverandør og applikationsleverandører forsøger efter bedste evne at forebygge og modarbejde sådanne angreb.

Opbevares elektroniske dokumenter udenfor Selvstyrets IT-systemer, er disse ikke nær så sikre. Opbevares de f.eks. på en USB, kan de forsvinde ved simpelt tyveri eller ganske enkelt bare blive væk. På en af Selvstyrets arbejdsstationer er risikoen for, at informationerne også forsvinder høj. Når en arbejdsstation skrottes, destrueres harddisken uden at nogen har haft adgang til indholdet.

At opbevare elektroniske dokumenter udenfor Selvstyrets IT-systemer medfører måske nok, at fremmede magter eller andre kriminelle ikke kan få adgang til oplysningerne. Men risikoen for, at informationerne går tabt er omvendt meget høj.

Inussiarnersumik inuulluaqqusillunga
Med venlig hilsen

Doris Jakobsen