Skatteankestyrelsen

Databeskyttelse og Informationssikkerhed

Skatteankenævn
November 2023

Agenda

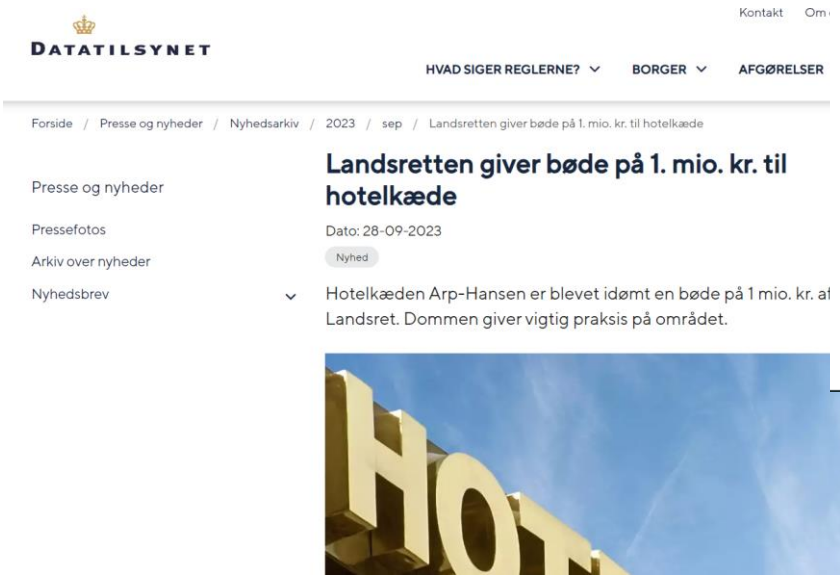
1. Et par hurtige spørgsmål
2. Organisering og kontekst
3. Databeskyttelse
4. Informationssikkerhed
5. Informationssikkerhedshåndbogen
6. Konkrete opmærksomhedspunkter
7. Afrunding

Et par indledende spørgsmål

Synes jeg, at informationssikkerhed og databeskyttelse er rigtig spændende – eller er det lidt kedeligt ?

Synes jeg, at informationssikkerhed og databeskyttelse er blevet mere eller mindre vigtigt gennem den senere tid ?

Virkeligheden som påvirkningsfaktor



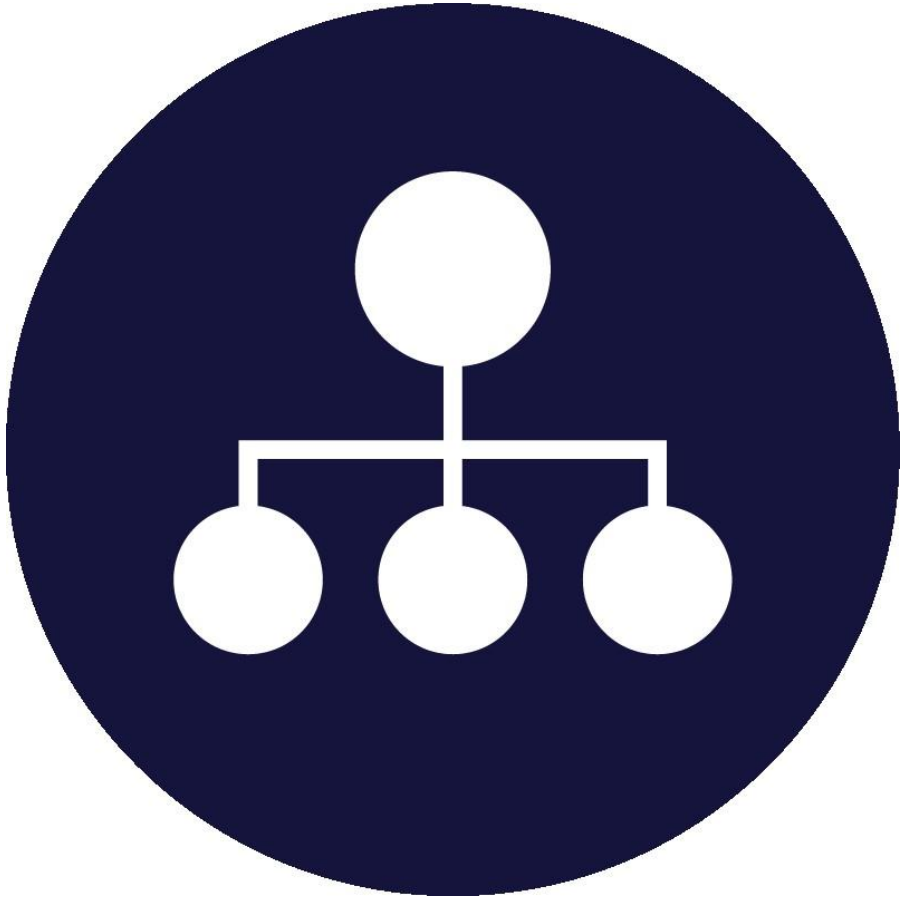
Hvad skal vi få ud af i dag?

Grundlæggende om databeskyttelse og informationssikkerhed

- Basisinformation om databeskyttelse og informationssikkerhed i forbindelse med dit hverv som medlem af skatteankenævn
- Lidt om organiseringen i forhold databeskyttelse og informationssikkerhed
- Forståelse af, at databeskyttelse drejer sig om beskyttelse af fysiske personers data, mens informationssikkerhed handler om at sikre og beskytte informationer på ethvert plan både fysisk og teknisk. Det er to selvstændige emner, men der altså også et klart overlap mellem de to emner
- Væsentlige opmærksomhedspunkter for dig, og hvor du kan få hjælp, hvis du har spørgsmål eller oplever et brud på persondatasikkerheden eller informationssikkerheden

Organiseringen

Databeskyttelse og informationssikkerhed

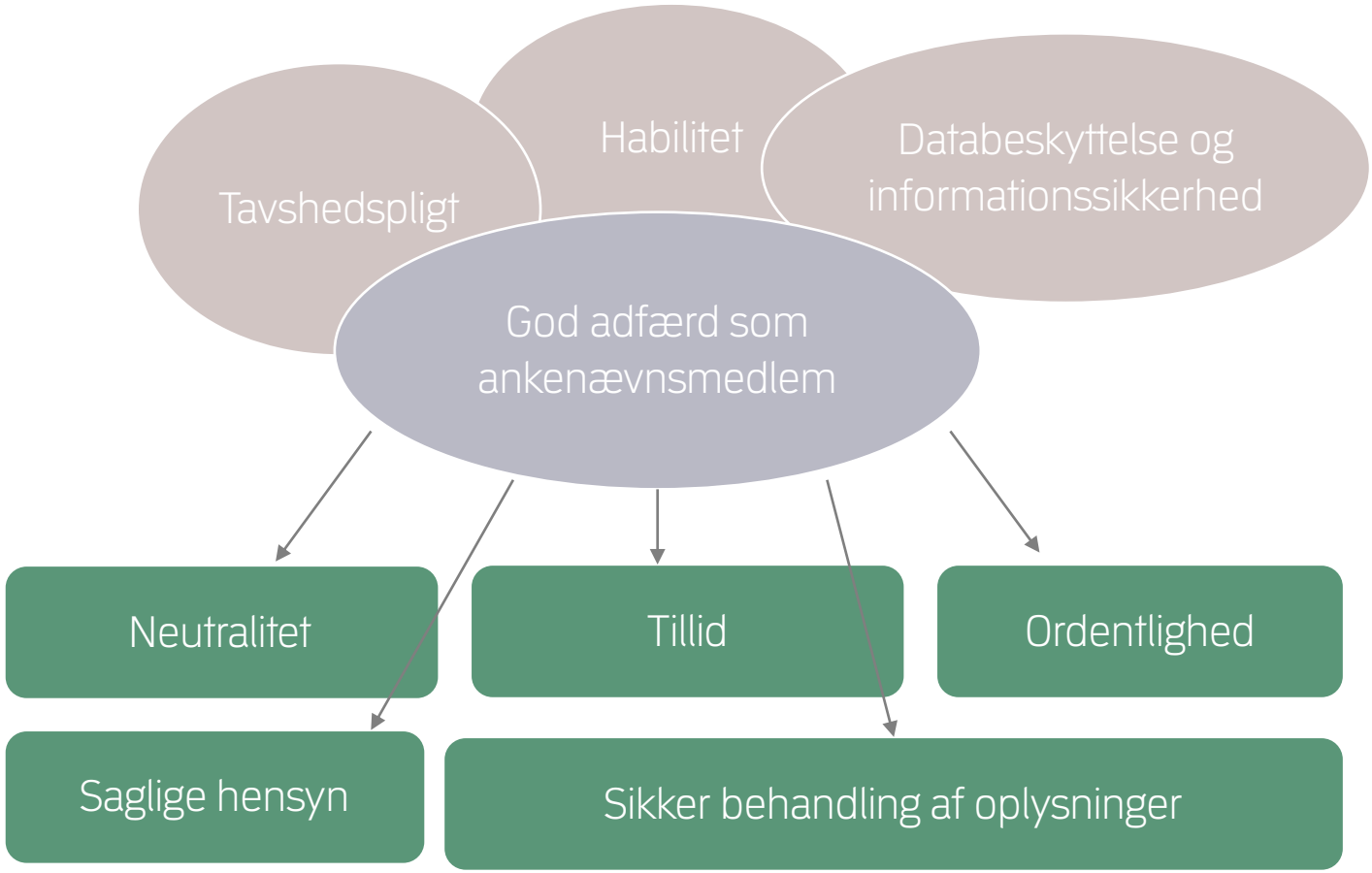


- Borgerne og virksomhederne skal have tillid til, at deres oplysninger behandles på en sikker måde
- Du skal som medlem af skatteankenævnet overholde reglerne om databeskyttelse og informationssikkerhed
- Som sekretariat for skatteankenævnet, hjælper Skatteankestyrelsen selvfølgelig også med databeskyttelse og informationssikkerhed
- Databeskyttelse er placeret i Databeskyttelsesteamet, som har databeskyttelseskoordinatoren som medlem. Teamet er i kontoret Generel Jura i Skatteankestyrelsen
- Informationssikkerhed er placeret hos informationssikkerhedskoordinatoren, som er i kontoret Digitalisering i Skatteankestyrelsen

Rammen for arbejdet som nævnsmedlem som kontekst

Rammerne for arbejdet

- Også skatteankenævnsmedlemmer skal behandle borgeres informationer på en sikker måde
- Sikker behandling og god adfærd er afgørende for, at borgerne har tillid til det arbejde, der udføres i skatteankenævnene
- Reglerne om databeskyttelse og informationssikkerhed gælder for arbejdet i skatteankenævnene og er en del af rammen for arbejdet



Databeskyttelse – også kaldet GDPR

Vi skal beskytte personoplysninger, vi får kendskab til via arbejdet

- Databeskyttelse kaldes ofte også GDPR – efter det engelske navn for databeskyttelsesforordningen (Generel Data Protection Regulation)
- Da klagesagerne næsten altid indeholder personoplysninger, så vil dit hverv med at deltage i afgørelsen af sagerne reelt altid indebære, at der sker en behandling af personoplysninger omfattet af databeskyttelsesforordningen
- Databeskyttelsesforordningen opererer med en meget bred definition af personoplysning og skelner mellem to typer af personoplysninger

Databeskyttelse – hvad er en personoplysning?

Enhver form for information om identificeret eller identificerbar fysisk person

Altså enhver form for information om identificeret eller identificerbar fysisk person

- Fx navn, cpr.nr., adresse, nummerplade, ip mv.

Man bruger også begrebet personhenførbar.

- Fx oplysninger vedrørende interessentskaber med fysiske personer som deltagere, da oplysningerne kan henføres direkte til den fysiske person bag interessentskabet.

- Der er to typer af personoplysninger:
  - Almindelige personoplysninger (GDPR art. 4, nr. 1)

    Fx navn og adresse
  - Følsomme personoplysninger (GDPR art. 9, stk. 1)

    Fx race, etnicitet, politisk, religiøst, helbredsoplysninger og oplysninger om seksuel orientering

Databeskyttelse – grundprincipperne

Databeskyttelsesforordningens artikel 5, stk. 1:

a	Lovlighed, rimelighed og gennemsigtighed	Personoplysninger skal behandles lovligt, rimeligt og på en gennemsigtig måde i forhold til den registrerede
b	Formålsbegrænsning	Personoplysninger skal indsamles til udtrykkeligt angivne og legitime formål og må ikke viderebehandles på en måde, der er uforenelig med disse formål
c	Dataminimering	Personoplysninger skal være tilstrækkelige, relevante og begrænset til, hvad der er nødvendigt i forhold til de formål, hvortil de behandles
d	Rigtighed	Være korrekte og om nødvendigt ajourførte
e	Opbevaringsbegrænsning	Opbevares på en sådan måde, at det ikke er muligt at identificere de registrerede i et længere tidsrum end det, der er nødvendigt til de formål, hvortil de pågældende personoplysninger behandles
f	Integritet og fortrolighed	Personoplysninger skal behandles på en måde, der sikrer tilstrækkelig sikkerhed for de pågældende personoplysninger.

Databeskyttelsesforordningens artikel 5, stk. 2:

"Den dataansvarlige er ansvarlig for og skal kunne påvise, at stk. 1 overholdes (ansvarlighed)."

Databeskyttelse – behandlingshjemmel og myndighedsudøvelse

Databeskyttelsesforordningens artikel 6, stk. 1, litra e:

"Behandling er kun lovlig, hvis og i det omfang mindst ét af følgende forhold gør sig gældende:

[...]

e) Behandling er nødvendig af hensyn til udførelse af en opgave i samfundets interesse eller som henhører under offentlig myndighedsudøvelse, som den dataansvarlige har fået pålagt."

Databeskyttelse – kravet om ansvarlighed

Databeskyttelsesforordningens artikel 24, stk. 1, 1. pkt.:

"Under hensyntagen til den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder gennemfører den dataansvarlige passende tekniske og organisatoriske foranstaltninger for at sikre og for at være i stand til at påvise, at behandling er i overensstemmelse med denne forordning."

Databeskyttelse - Konsekvenser af kravet om ansvarlighed

Myndighederne skal sikre og kunne påvise, at behandling sker i overensstemmelse med databeskyttelsesreglerne. Der er ikke nok, at behandlingen rent faktisk foregår korrekt. Det er et selvstændigt krav, at det skal myndigheden også kunne påvise.

Myndighederne skal fastsætte, implementere og vedligeholde politikker om beskyttelse af personoplysninger.

Skriftlig dokumentation er derfor også en forudsætning for ansvarlighed.

"Kravet om at føre fortegnelser over behandlingsaktiviteter hænger – som nævnt ovenfor – i vidt omfang sammen med forordningens princip om ansvarlighed ("accountability"). Ansvarligheden kommer til udtryk ved, at den dataansvarlige både skal efterleve forordningens regler og samtidig være i stand til at påvise, at dette rent faktisk er tilfældet."
Datatilsynets tilsyn, j.nr. 2018-423-0020.

"Det følger af databeskyttelsesforordningens artikel 24, stk. 1, at den dataansvarlige, under hensyntagen til den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder, skal gennemføre passende tekniske og organisatoriske foranstaltninger for at sikre og for at være i stand til at påvise, at behandling er i overensstemmelse med denne forordning."
Alvorlig kritik af dataansvarlig grundet manglende sikkerhedsforanstaltninger ved hackerangreb i Datatilsynets afgørelse,
j. nr. 2021-441-10210

Vigtigheden af skriftlige retningslinjer og dokumentation

KONKLUSION

Rigsrevisionen har undersøgt, hvordan 8 statslige institutioner behandler fortrolige oplysninger om personer og virksomheder i 11 udvalgte it-systemer. Rigsrevisionen finder det utilfredsstillende, at institutionerne ikke beskytter fortrolige oplysninger om personer og virksomheder tilstrækkeligt.

Når en institution ikke beskytter fortrolige oplysninger tilstrækkeligt, øger det risikoen for, at uvedkommende får kendskab til fortrolige oplysninger, og at oplysningerne kan misbruges. Manglende beskyttelse af fortrolige oplysninger kan desuden svække borgeres og virksomheders tillid til it-sikkerheden i den statslige forvaltning, hvilket kan blive en barriere for fortsat at digitalisere og effektivisere i staten.

Undersøgelsen viser, at ingen af de undersøgte institutioner efterlever alle de krav til behandling af fortrolige personoplysninger, som fremgår af sikkerhedsbekendtgørelsen, og som er en uddybning af persondatalovens bestemmelser. De undersøgte institutioner mangler i vidt omfang at opdatere interne retningslinjer, at kontrollere brugeradgange, at registrere medarbejdernes opslag og slette dem igen, at følge op på indgåede aftaler med eksterne databehandlere overholdes, og at føre tilsyn med, at interne sikkerhedsforanstaltninger overholdes. Selv institutioner som Danmarks Statistik, Rigspolitiet og SKAT, der er vant til at håndtere store mængder fortrolige oplysninger, har i de undersøgte systemer ikke efterlevet sikkerhedsbekendtgørelsens krav på flere punkter.

4. En statslig institution kan sikre oplysninger ved at gennemføre forskellige tiltag, der forbedrer it-sikkerheden. Det kan være gennem organisatoriske eller administrative tiltag som fx at udarbejde risikovurderinger og instrukser, som fastlægger forretningsgange og ansvar for it-sikkerheden og for kontrol og tilsyn. Det kan også være tekniske løsninger, der medvirker til at sikre, at kun medarbejdere med et arbejdsbetinget behov får adgang til oplysningerne. Desuden kan det være at sikre den fysiske bygning, hvor oplysninger behandles, mod uautoriseret adgang.

Kilde: Beretning om statens behandling af fortrolige oplysninger om personer og virksomheder (rigsrevisionen.dk)

Vigtigheden af skriftlige retningslinjer og dokumentation

Tabel 2. Retningslinjer for at sikre fortrolige personoplysninger i de undersøgte institutioner

	Arbejds-skade-styrelsen	Institut for Menneske-rettigheder	Danmarks Statistik	Forsvars-komman-doen	Rigspolitiet	SKAT	Social-styrelsen	Sundheds-styrelsen
Er der ret-ningslinjer for at sikre personop-lysninger?	●	●	●	●	●	●	●	●
Er retnings-linjerne op-dateret år-ligt?	●	●	●	●	●	●	●	●

● Ikke tilfredsstillende, da der forekommer væsentlige mangler.
● Delvist tilfredsstillende.
● Tilfredsstillende, men mindre mangler kan forekomme.

Kilde: Rigsrevisionen.

Det fremgår af tabel 2. at 5 ud af 8 institutioner (Arbeidsskadestvrelsen. Danmarks Statistik.

Kilde: Beretning om statens behandling af fortrolige oplysninger om personer og virksomheder (rigsrevisionen.dk)

Anmeld et brud på persondatabeskyttelsen

Hvis der sker et brud på persondatasikkerheden eller du har mistanke om, at der er sket et brud, så skal du reagere hurtigt

Anmeld brud på persondatasikkerhed

- Databeskyttelsesteamet i Generel Jura skal kontaktes hurtigst muligt, hvis der er sket brud eller er risiko for, at der er sket brud på persondatasikkerheden. Skriv til os på databeskyttelse@sanst.dk.
- Vi hjælper dig med at håndtere hændelsen.
- Databeskyttelsesforordningen indeholder en anmeldelsespligt til Datatilsynet ved brud på persondatasikkerheden. Bruddet skal være anmeldt inden for 72 timer, derfor er hurtig kontakt vigtig.

Hvis du opdager et brud eller risiko for brud på persondatasikkerheden, skal du handle med det samme

Skriv til **databeskyttelse@sanst.dk** og angiv:

- Dato og tidspunkt for bruddet
- Hvad der er sket og hvorfor
- Hvilke personoplysninger, der er lækket
- Konsekvenserne af bruddet
- Sagsnummer mv.

Databeskyttelsesteamet kvitterer for din mail hurtigst muligt. De indberetter bruddet og håndterer den videre proces.

Ring også til Generel Jura på **3376 0942.**

Fortæl om bruddet og gør opmærksom på, at du har skrevet til databeskyttelsesteamet.

Hvis du ***ikke*** modtager en kvittering på mail fra databeskyttelsesteamet inden for 1 time, og hvis du ikke kan få fat på Generel Jura over telefonen, skal du ringe til 7237 7777 og følge deres anvisninger.

Informationssikkerhed – overordnet

Vi skal beskytte informationer, som vi har ansvaret for

- ISO 27001 er egentlig en international ledelsesstandard til styring af informationssikkerhed. Et styringsværktøj, der hjælper til at beskytte informationer på en sikker og troværdig måde
- Alle statslige myndigheder skal følge ISO 27001 – det vil sige både Skatteankestyrelsen som sekretariat og skatteankenævn
- ISO 27001 stiller blandt andet krav om dokumenter med:
    - Beskrivelse af roller, ansvar og beføjelser, beskrivelse af risikovurderingsproces og risikohåndteringsproces, og dokumentation af uddannelse
- Standarden bidrager til at skabe tillid til den enkelte myndigheds arbejde med informationer, og et struktureret og dokumenteret arbejde med informationssikkerhed

Informationssikkerhed – grundprincipper

Grundlæggende informationssikkerhed

- Informationssikkerhed skal bevare fortrolighed, integritet og tilgængelighed af information ved hjælp af en risikostyingsproces og sikre, at interessenter har tillid til, at risici håndteres på en ordentlig måde

Fortrolighed
Beskyttelse af informationer mod uautoriseret videregivelse eller adgang.

Integritet
Beskyttelse af informationer mod uautoriseret ændring eller ødelæggelse, også utilsigtet ødelæggelse samt sikring af informationers nøjagtighed og pålidelighed.

Tilgængelighed
Beskyttelse af informationer mod uautoriseret adgangsforbud for de personer, som har retmæssig adgang.

Informationssikkerhed – det skriftlige

Skatteministeriets koncernfælles informationssikkerhedshåndbog som dokumentation for procedurer

- Informationssikkerhed handler altså om at sikre og beskytte information, så vi sikrer fortrolighed, pålidelighed og tilgængelighed. Det betyder, at vi skal have kontrol med, hvem der har adgang til og kan ændre informationerne, og vi skal sikre, at vigtige data er tilgængelige

- Alle har et ansvar for at værne om informationerne ved at følge retningslinjerne i den koncernfælles håndbog om informationssikkerhed

- Informationssikkerhedshåndbogen er grundlæggende et centralt omdrejningspunkt for ***dokumentationen*** både i forhold til:

    - Databeskyttelsesrettens accountability

    - Informationssikkerhedens dokumentationskrav

Indhold i Informationssikkerhedshåndbogen

Retningslinjer

- Informationssikkerhedshåndbogen indeholder skriftlige retningslinjer, der bidrager til en sikker behandling af informationer

- Informationssikkerhedshåndbogen er udtryk for:
  - Allerede gældende regler og principper
  - Sund fornuft
  - Bidrager til beskyttelse af borgeres oplysninger og egne oplysninger

- Informationssikkerhedshåndbogen indeholder bl.a. eksempler på:
  - Hvordan sikres informationerne bedst muligt, fx ved brug af gode adgangskoder mv.
  - Hvordan spottes og håndteres mistænkelige mails
  - Hvordan bruges internettet på en sikker måde

Informationssikkerhedshåndbogen er tænkt koncernfælles

Informationssikkerhedshåndbogen er faktisk tænkt at gælde for alle:

- Medarbejdere, samarbejdspartnere, leverandører, vikarer/eksterne konsulenter mv.
- Den er egentlig tænkt ud fra, at det afgørende er, at personen arbejder med data/informationer/oplysninger i koncernens IT-systemer og på koncernens udstyr – uafhængigt af personens nærmere tilknytning til koncernen
- Altså ikke tænkt som afgørende, om personen fx er en almindelig medarbejder, en leverandør eller fx et ankenævnsmedlem
- Reelt udtryk for, at hele tankegangen tager udgangspunkt i data/informationer/oplysninger – ikke i myndigheder/personer/virksomheder, som ellers typisk netop er det klassiske udgangspunkt
- MEN – det er også tydeligt, at Informationssikkerhedshåndbogen primært er målrettet egentlige medarbejdere

Informationsikkerhedshåndbogen – et par opmærksomhedspunkter

Lige et par væsentlige ting

- Når du læser håndbogen, skal du derfor ikke lade dig forvirre af, at ordene ”ansatte” og ”medarbejder” bruges. Det er håndbogens principper, der er det vigtige, og håndbogens principper er relevante for dig og for dit arbejde i skatteankenævnet
- Det er samtidig vigtigt at være opmærksom på, at der for medlemmer af skatteankenævn gælder undtagelser
- Beskrivelsen af hjemmearbejde på side 15 skal fx læses i lyset af, at det er principperne, der er det vigtige. Beskrivelsen passer således ikke på alle punkter til situationen som medlem af skatteankenævn
- Se forsiden til Informationssikkerhedshåndbogen for medlemmer af skatteankenævn

Informationssikkerhedshåndbogen – et par opmærksomhedspunkter

Lige et par væsentlige ting – forsat

- Det betyder blandt andet, at du skal sikre,
  - at data altid opbevares i Skatteministeriets systemer og IT-udstyr
  - at dit udstyr altid er opdateret
  - at du anvender koncernens Citrix-løsning, hvis du arbejder via en privat pc
  - at du låser din pc/iPad, når du forlader den og opbevarer fysiske dokumenter, så andre ikke kan få adgang til dem
  - at du på grund af risiko for virus er varsom med at klikke på links og vedhæftede filer i mails, som du får tilsendt, hvor du ikke kender afsenderen

Phishing – rapportér phishing

De seks tegn på at du har modtaget en phishingmail

1. Du har ikke nogen relation til afsenderen.

2. Afsenderadressen i mailen ser mistænkelig ud.

3. Der er sprog- og stavefejl.

4. Afsenderen kræver, at du videregiver dine personlige oplysninger.

5. Adressen i et medsendt link ser underlig ud.

6. Afsenderen er en leder som beder dig gøre noget usædvanligt.

- Hvis du modtager en mistænkelig mail, skal du rapportere denne ved at klikke på "Rapportér phishing" i båndet i højre hjørne i Outlook.

- Hvis du har åbnet en fil eller klikket på et link i en mistænkelig mail, skal du straks kontakte 5x7 (tlf. 72 37 77 77).

Hvad skal jeg være opmærksom på?

Hackere bliver bedre og bedre til at lave phishingmails, som er svære at gennemskue. Så for at sikre, at ovenstående udvikling fortsætter i den positive retning, er der en række gode råd, som du altid skal følge:

1. Klik aldrig på links i mails, hvis du er det mindste i tvivl.

2. Benyt i stedet knappen "rapportér phishing" i Outlook, så 5x7 hurtigt kan stoppe en eventuel hændelse.

3. Rapportér hellere mails én gang for meget end én gang for lidt.

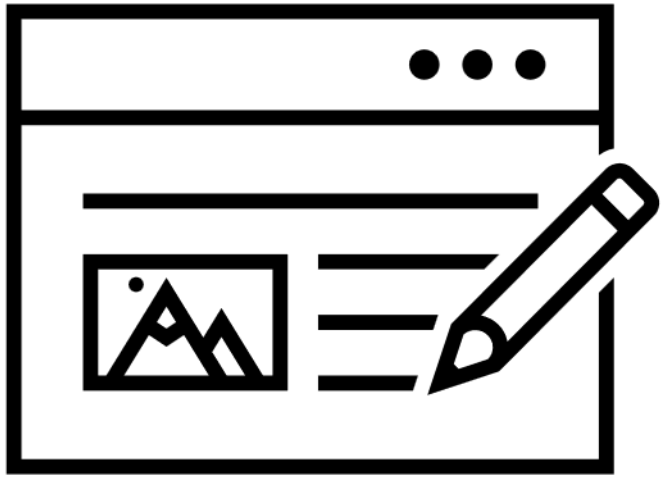
4. Hvis du får klikket på et link og mistænker phishing, så kontakt 5x7 med det samme, så de kan minimere skaden.

Anmeld et brud på informationssikkerheden

Hvis der sker et brud på informationssikkerheden eller du har mistanke om, at der er sket et brud, så skal du reagere.

Anmeld brud på informationssikkerheden – sikkerhedshændelse:

- Du skal anmelde det potentielle brud eller bruddet på informationssikkerheden til den koncernfælles IT-support på tlf. 72 37 77 77 og følge deres anvisninger
- Du bør også gerne orientere nævnsbetjeneren om din anmeldelse



Kritik – og det der er værre

Sundhedsdatastyrelsen får kritik af Datatilsynet

En sag om manglende kontrol med opbevaring af personoplysninger i e

17 sep. 2021 kl. 12:51

usikkert miljø, udløser nu kritik af Sundhedsdatastyrelsen.

Nu skal politiet efterforske, om der er grundlag for at rejse sigtelse. Arkivfoto: Louise Koustrup

1/1

Datatilsynet har politianmeldt Region Syddanmark og indstillet, at den bør få en bøde på 500.000 kroner på grund af sløseri med personoplysninger. Det skete også i juli. Regionen tager beslutningen til efterretning.

(Foto: Povl D. Rasmussen)

Medarbejderes telefoner pivåbne: Datatilsynet melder kommune til politiet for mangel på 'helt basale sikkerhedsforanstaltninger'

Datatilsynet vil have Lolland Kommune til at betale bøde for at mangle 'helt basale sikkerhedsforanstaltninger' i medarbejdernes brug af telefoner og tablet-computere.

11. august 2022 kl. 14.27

DAN

Tak for jeres opmærksomhed - meget værdsat