5 trinn for å komme igang med GDPR

1. Trinn: Handlingsplan for GDPR arbeidet og internkontrollsystemet

I handlingsplanen din skal du ha oversikt over hva du må gjøre nå og hva du kan gjøre senere iforhold til internkontrollsystemet. Du skal lage en liste over arbeidet du må gjøre rett og slett, og alt må få en dato og ansvarlig person !

(Selve oppsettet av og gjennomføring av internkontrollsystemet gjør vi i trinn 4 - det er en overordnet plan og skiller seg fra handlingsplanen som skal være konkret og detaljert)

A: Hva skal jeg finne ut

Du må finne ut blandt annet om

- personopplysninger brukt i firmaet eller samlet inn av eller gjennom ditt firma
- personopplysninger om ansatte
- hvilke type opplysninger er det - er noen sensitive
- om du er både behandlingsansvarlig og databehandler - eller bare behandlingsansvarlig
- Hvilke firmaer oppbevarer data for dere
- Har dere en skyløsning eller backup løsning
- Finnes det papirer som står åpent tilgjengelig for alle som inneholder sensitiv informasjon
- Hvilke type informasjon finner jeg på eposter, hardisker og ipader i mitt firma - finnes det personopplysninger der
- Hvordan sikrer jeg at eposter som sendes ut er "lovlige"
- O.s.v.

(i en slik liste vil det også stå mange ting som du kanskje ikke får gjort noe mer før om noen år, men det kan du bestemme senere gjennom risikoanalysen som du skal gjøre i trinn 5)

B: Hvordan finner jeg denne informasjonen.

Sett deg ned sammen med noen i bedriften din for å finne ut hvor er det dere oppbevarer personopplysninger.

Finn ut om det er noen opplysninger dere registrerer som er sensitive - altså at de handler om helse, eller andre konfidensieller ting. Det at en opplysning er sensitiv kan også være at den sier om du er medlem i et trossamfunn, hvilken organisasjon du tilhører og hvilken legning du har.

Veldig mange arbeidsgivere har noen sensitive opplysninger på sine datamaskiner i forbindelse med sykefravær hos ansatte. Det er viktig at disse opplysningene behandles med høyere sikkerhet enn vanlig personopplysninger.

Uansett hvilke typer personopplysninger det er - om de er "vanlige" eller sensitive - så skal du skaffe en oversikt over hvilke opplysninger det er.

Typisk har du opplysninger om

Kunder, ansatte, samarbeidspartnere, eiere og andre mennesker du er i kontakt med knyttet til driften av firmaet.

Hvis du har et kontaktskjema på din nettside hvor en person kan gi deg sitt navn , telefonnr og epostadresse så samler du inn personopplysninger i tillegg til å ta vare på de du trenger.

Samle alle typer av kategorier du oppbevarer:

Navn, telefonnummer, adresse, epost os.v

Trinn 2: Du må ha en personvernerklæring

Alle bedrifter som samler inn personopplysninger må ha en personvernerklæring.

Jeg skal forsøke å være kortfattet her, men akkurat dette med personvernerklæring er lett å bli noe som man gjøre uten virkelig å tenke igjennom utfordringene.

Det er viktig at du ikke skriver noe i erklæringen som ikke stemmer med din praksis - og på den måten risikerer å gjøre en skikkelig feil (se bilde)

Personvernerklæringen skal i detalj forklare hvordan du sikrer at de opplysningene du samler inn blir forsvarlig lagret og ikke brukt av andre.

Jeg anbefaler deg å se igjennom den gjennomgangen vi har laget på www.pvern.no som omhandler personvernerklæring.

Det kan være mange detaljer der som du ikke har tenkt på før.

Det de fleste gjør feil på er rutiner rundt å innhente samtykke. I virkeligheten er det nemlig slik at ikke alle trenger å hente inn samtykke. Hvis du har kunder som du har hatt i mange år så trenger ikke de å sende inn samtykke for å fortsette å få informasjon fra deg.

En annen utfordringer er om den bedriften du har websider / regnskap / backup hos har laget en databehandleravtale med deg ?

https://www.pvern.no/skrive-personvernerklaering-23048s.html?show=4

Trinn 3 : Du trenger en databehandleravtale

Alle bedrifter som lagrer noe informasjonn om personer hos andre bedrifter må ha databehandleravtale med dem.

En slik avtale sikrer at de ikke misbruker opplysninger du som behandlingsansvarlig har gitt dem, og den sikrer at opplysningene blir oppbevart sikkert og i henhold til GDPR lovverket.

Det er mange vanskelige detaljer i en slik avtale og fortsatt er bransjen usikker på endel av de vanskelige detaljene knyttet til kryptering, sikkerhet og godkjennelser på ulike nivåer.

Hvis du tenker deg om så ønsker jo du ikke selv at alle eposter du sender ut skal være like vanskelige å åpne som de som sendes gjennom Altinn eller fra bankens sikre systemer.

Foreløpig ønsker vi så mye åpehent som mulig, men det er mulig at verden snart blir så usikker at alle vil ønske å sikre selv vanlige eposter mellom kunder og brukere.

Databehandleravtalene vil derfor blir redigert og endret i årene fremover, men det er uansett viktig å ha en avtale for å starte.

Se mer detaljer om denne avtalen her:

https://www.pvern.no/databehandleravtale-gdpr-hjelp-23155s.html?show=5

Trinn 4: Du må starte et interkontrollsystem

For at din virksomhet skal jobbe lovlig med personopplysninger så må du ha et interkontrollsystem i din bedrift for GDPR.

Mange lurer på hva dette er og kvier seg for å sette igang noe som de tenker vil kreve en advokat eller konsulent for å sette igang.

For det første: Husk at en advokat kan gi deg gode juridiske råd om de vanskelige avveiningene i GDPR arbeidet. Det er kun de som har lov å gi juridiske råd. Allikevel så er det slik at du som eier av en bedrift stort sett klarer deg fint med å lære av firmaer slik som oss hvordan GDPR arbeidet skal utføres. Arbeidet kan du utføre selv etter de oppskrifter vi gir, og hvis du får en personver utfordringen i arbeidet så kan du spørre en advokat om råd i den saken.

Internkontrollsarbeidet dreier seg om 4 faser - alle disse skal gjøres hvert år så i praksis må dere sette av tid til 4 møter i bedriften spredt utover hele året:

(Mye av punktene her har sammenheng med info du fant frem til handlingsplanen din i trinn 1, men internkontrollsystemet ditt er på et mer overordnet plan og skal hele tiden "snakke med" handlingsplanen og risikoanalysen som vi ser på i trinn 5 .

Igangsette (Januar hvert år)
• ta initiativ til arbeidet
• informere, medvirke og motivere
• sette mål og beskrive ansvar og myndighet
• organisere og planlegge innføringen

Kartlegge (Februar- mars hvert år)
• skaffe oversikt over aktuelle lover og forskrifter
• kartlegge eksisterende rutiner for GDPR
• systematisere og oppbevare dokumenter
• kartlegge problemområder

Planlegge og prioritere tiltak (juni - okt)
• lage handlingsplan for gjennomføring

Følge opp (nov - des hvert år)
• gjennomføre tiltak

• rette opp feil og mangler
• gjøre forbedringsarbeidet til en naturlig del av den daglige driften
• foreta jevnlig gjennomgang

Se eksempel på gdpr.romerike.com

Trinn 5: Risikoanalyser

Hele GDPR arbeidet dreier seg om å ta personvernet på alvor. I den forbindelse er det nødvendig at du er sikker på at ikke noen opplysninger kan forsvinne eller bli delt med andre.

I den verden vi nå lever i med hackerangrep og virus som er smarte så vil det være nødvendig med stadig å gjennomføre risikoanalyser.

Mange analyser kan dreie seg om rutiner i firmaet i forhold til oppbevaring av opplysninger, mens andre er mer avanserte knyttet til oppbevaring på data, i nett og på websiden din.

Vi oppfordrer alle til å få hjelp til å sikre opplysningene på en god måte gjennom viruskontroll, brannvegg, men samtidig også oppbevare gode backup av systemene.

I den senere tid har det også vært tilfeller hvor folk har bedt om penger for å gi tilbake tilgangen til bedriftens IT systemer.