

Personvern i styrerommet

Det er bare 13 måneder igjen til EUs nye og inngripende personvernregler trer i kraft. Daglig leders og styremedlemmers personlige ansvar har vært lite diskutert.

I mai 2018 trer EUs nye personvernregler i kraft. Advokat Eva Jarbekk omtalte gruppesøksmål i en kronikk i DN den 3. april. Daglig leders og styremedlemmers personlige ansvar har vært lite diskutert.

Datasikkerhet og personvern har ikke vært diskutert mye i styrerommene. Ansvaret for dette har vært overlatt til CTO og IT-avdelingen. Med gjennomgripende digitalisering og en massiv økning av datakriminalitet, er det på høy tid at styrer og ledelse våkner. Med EUs nye personvernregler - General Data Protection Regulation (GDPR) - skjerpes styrets plikter, og dermed muligheten for å komme i ansvar.

Ledelsen og styret i norske virksomheter har etter aksjeloven ansvar for forsvarlig drift. I tillegg til tradisjonell oppfølging, krever GDPR at tilfredsstillende tekniske og organisatoriske tiltak for å sikre personvernet iverksettes. Personvernet omfatter ansatte, kunder, leverandører, pasienter, medlemmer, borgere m.m.

GDPR er blitt kjent for sitt bøtenivå. Bøtenivået er blitt skjerpet for at ledelsen skal våkne og ta grep. Dersom ledelsen og styret sørger for etterlevelse, reduseres derfor sjansene for høye bøter kraftig. GDPR artikkel 83 sier uttrykkelig at bøter ved databrudd skal fastsettes etter overtredelsens grovhet - og hvilke sikringstiltak virksomheten har iverksatt.

Men de høye bøtene bør ikke være den viktigste grunnen til å etterleve reglene. Like viktig er risikoen for tap av virksomhetens omdømme. Ikke bare er eksemplene vi har sett i media angående bruk av apper og hacking alvorlige - i forrige uke skrev Digi om brukernes risiko ved at alt, både bilbrems, fengselsdører og fly, kan hackes. Samtidig avslørte også TV 2 Hjelper deg at et antall kundeklubber systematisk behandler personopplysninger ulovlig. Risikoen for omdøm-



Å unnlate å beskytte seg mot dataangrep og tap kan anses som uforutsigelig opptreden fra ledelsen og styret, særlig når kravene er strenge og risikoen er godt kjent, skriver innleggsforfatterne.

Foto: Hampus Lundgren

Innlegg Kristian Foss og Kristin Haram Førde



metap og erstatningskrav er høy ved slike hendelser.

Å unnlate å beskytte seg mot dataangrep og tap kan anses som uforutsigelig opptreden fra ledelsen og styret, særlig når kravene er strenge og risikoen er godt kjent.

Hvordan skal virksomheten ta sitt ansvar?

Skaff deg en oversikt over hva GDPR og datasikkerhet betyr for din virksomhet. Selv om GDPR reiser en rekke juridiske spørsmål, er etterlevelse i stor grad en logistikkoperasjon. Operasjonen må organiseres godt, for tiden er knapp frem til mai 2018, når GDPR trer i kraft.

I første fase bør du sette sammen et lag, med én ansvarlig person som rapporterer til daglig leder og styret. Du som styremedlem eller daglig leder trenger ikke å være ekspert i personvern, men må sørge for relevant rådgivning.

I andre fase bør dere kartlegge



Kristian Foss,
personvernadvokat i
Bull og Co advokat-
firma.



Kristin Haram Førde,
personvernadvokat i
Bull og Co advokat-
firma.

dagens situasjon, og vurdere hva virksomheten mangler etter de nye reglene. Hvilke nye rutiner må på plass?

Den tredje fasen innebærer å utarbeide nødvendige rutiner: Risikovurderinger, compliance-mekanismer, handlingsplaner ved databrudd, katastrofeberedskap og retningslinjer for innebygget personvern, for å nevne noen.

I fase fire implementeres rutinene teknisk og organisatorisk. Sørg for at rutinene blir kjent, at virksomheten og underleverandører utvikler kultur for godt personvern, og at virksomhetens avtaleverk reflekterer dette.

Påse videre at personvern og datasikkerhet kommer inn på styrets årshjul og inn i styreinstruksen. Fordi ikke-personlige data kan være like viktige som personlige data, bør rutinene innlemmes i det generelle kvalitets- og sikkerhetsarbeidet.

Sist, men ikke minst, forsikre deg om at virksomhetens forsikringer dekker denne nye virkeligheten. Gjenoppretting av

EUs personvernforordning

● Trer i kraft i 2018 og gjelder også i Norge.

● Alle virksomheter som samler inn eller bruker personopplysninger om EU/EØS-borgere må følge reglene.

Hovedtrekk

● Alle skal ha en forståelig personvernerklæring.

● Alle skal vurdere risiko og personvernkonsekvenser.

● Alle skal bygge personvern inn i nye løsninger.

En egen «sjekklister» for innebygd personvern er opprettet.

● Mange bedrifter må få eget personvernombud.

Gjelder offentlige virksomheter og virksomheter som håndterer personopplysninger i stor skala.

● Gjelder også virksomheter utenfor Europa

Dersom man selger varer eller tjenester til Europeere.

● Også underleverandører som håndterer eller oppbevarer persondata for ansvarlige virksomheter får nye regler.

● Den nye loven oppfordrer til samarbeid om bransjenormer på personvernområdet.

● Krav til avvikshåndtering
Alle avvik som kan medføre risiko for privatpersoner skal meldes til Datatilsynet innen 72 timer.

● Alle må kunne oppfylle borgernes nye rettigheter
EU/EØS-borgere får nye rettigheter med GDPR, blant annet retten til å bli glemt, rett til å sette begrensninger på hvordan personopplysninger brukes.

● Kilde: Datatilsynet

data, sikring og varsling av tusenvis av personer ved databrudd kan bli kostbart. Det samme gjelder tiltak for å redusere skaden på omdømmet og juridisk bistand.

Tiden er knapp. Passivitet er risikofylt. Begynn nå.

Kristian Foss og Kristin Haram Førde, personvernadvokater i Bull & Co advokatfirma og står bak Personvernfabrikken.no.

På nattbordet Øyvind Horpestad



Alder: 47
Stilling: CEO, NRC Group

- Nå må jeg tenke meg om, jeg er nok ganske kjedelig. Jeg har noen bøker der, og et nettbrett og noen aviser.

- Blir det raskt slik at nettbrettet trekker mer enn bøkene?

- Jeg liker å lese og har lest mye, men jeg er blitt dårligere og dårligere til å lese bøker. Det har noe med hverdagen å gjøre, det blir fort mange barnebøker i stedet.

- Du er i stort selskap. Hva er titlene på bøkene?

- Jeg har snappet med meg den nye til Jo Nesbø, «Tørst». Og så har jeg en gammel favoritt, Giovanni Guareschi «Don Camillo». Den tar vel utgangspunkt i en avisføljetong som siden er blitt bøker, med humoristiske fortellinger fra etterkrigstiden i Italia, og med konflikter mellom prestene, borgerskapet og kommunistene.

- Mens alle andre leser Elena Ferrante, nærmer du deg nyere italiensk historie fra en annen vinkel!

- Jeg kom over den en gang da jeg var i tyveårene. Det er morsomme fortellinger om viktige ting, om hvordan ellers gode standpunkter kommer til kort hvis man er for steil. Temmelig lokalt perspektiv, men med allmenngyldige temaer.

- Noen bøker som har betydd spesielt mye for deg?

- Jeg vokste opp på 1980-tallet, og det er en del norske forfattere som farget ungdommen. Ingvar Ambjørnsens «Hvite niggere» og «Den siste revejakten», så klart. Og Lars Saabye Christensen har nok hatt en betydning.

- Du nevnte barnebøker. Gjenskaper du din egen glade oppvekst eller søker du deg til nye ting?

- Fjortenåringen er nok ikke så interessert i at jeg leser for ham lenger, men jeg har også en på tre og en på seks. Og hun på seks har begynt på skolen og har skjønnet hvordan hun kan få lesetunden med «Detektivbyrå nr 2» til å vare tre ganger så lenge. Nemlig ved at hun leser selv.

- Brains. Hvordan er fordelingen mellom klassisk barnelitteratur og det nye?

- Det er lett til at man tyr til det man selv var glad i. Men med nye tider er det nye ting som fenger, og det trenger jo ikke være dårligere, det kan til og med være bedre.

- Men i påsken holdes tradisjonen med krim?

- Ja, da blir det «Tørst».