3M | The experts in screen privacy.

# GDPR-beredskap
# Vanlige spørsmål

## Enza Iannopollo, Forrester Research

Enza er analytiker i sikkerhets- og risikoteamet og autorisert spesialist på personvern (CIPP/E). Hos Forrester dekker hun områdene databeskyttelse, personvern, analyseteknikker og tingenes internett med fokus på innvirkningen av regelverk og teknologiene de bygger på.

GDPR er en av de viktigste endringene innenfor personvernregler på 20 år. Det etablerer hvordan organisasjoner på løpende basis må håndtere de personlige dataene til kunder, medarbeidere og forretningspartnere. 3M satt nylig i samtaler med Enza Iannopollo fra Forrester Research for å drøfte samsvarsprogrammene for sikkerhetstiltak, retningslinjer og personvern som mange organisasjoner oppretter for å overholde regelverk som GDPR. Enza ga innsikt i beredskapen på arbeidsplassen og understreket behovet for fysiske sikringstiltak for å beskytte mot personverntrusler.

### Hva står på spill?

Organisasjoner kan bøtelegges med opptil 4 % av årlig global omsetning eller

€20 M FINE

Her er hva hun hadde å si:

**Sp. Er arbeidsstyrkene klare til å fungere i samsvar med GDPR?**

**Sv.** Tallene våre viser at kun ett av tre selskaper globalt er klare til å overholde EUs generelle personvernforordning (GDPR, General Data Protection Regulation). Da håndhevingen av GDPR starter den 25. mai 2018, er det klart at mange organisasjoner må jobbe raskt for å fullføre forberedelsene sine.

Vi ser særlig at bedrifter sliter med å innfri kravene til implementering og dokumentasjon av opplærings- og bevisstgjøringsprogrammer innen personvern for sine medarbeidere. Tilsynsmyndighetene i EU har indikert at disse programmene er grunnleggende for GDPR-samsvar. Samtidig har vi funnet at organisasjoner som innfrir dette kravet, har forbedret personvernkulturen i selskapet og etablert anbefalte praksiser som noen ganger er mer omfattende enn kravene fra tilsynsmyndighetene.

**Sp. Er selskaper i bestemte regioner bedre forberedt enn andre?**

**A.** 34 prosent av amerikanske selskaper sier at de er klare, sammenlignet med 26 prosent av selskapene i Europa.[1] Selskaper som ikke er i samsvar med GDPR – enten de er klar over dette eller ikke – påtar seg en stor forretningsrisiko. Selskaper som tror de er klare, men ikke er det, tar en enda større risiko.

Det er interessant å legge merke til at flere selskaper i USA mener de er klare, sammenlignet med Europa. Dette har å gjøre med den eksterritoriale virkningen av GDPR. Regelverket gjelder alle selskaper – uavhengig av hvor de befinner seg – som behandler eller innehar persondata for EU-borgere. Dette betyr at ikke bare europeiske selskaper, men også mange selskaper med hovedkvarterer i USA vil måtte overholde disse strenge personvernreglene.

Vi mistenker at en overfladisk lesning av reglene sammen med villedende og ubegrunnede forventninger om svak håndhevelse av GDPR, kan påvirke selskapenes oppfatninger om beredskapen deres.

**Sp. Hvilke fysiske sikkerheter og personvernsikringer kreves av GDPR?**

**Sv.**GDPR er et prinsippbasert regelverk.Dette betyr at tilsynsmyndighetene ikke utstyrer organisasjoner med et sett med definitive tiltak som må følges. I stedet bør organisasjoner tenke på GDPR-krav som en type «ønsket tilstand» for hvordan de håndterer data. Det betyr også at organisasjoner må identifisere og vurdere spesifikke risikoer som de må utbedre for å samsvare med GDPR-krav.

Når bedriftene identifiserer risikoer, må de ta hensyn til risikoer forbundet med databehandling, særlig de risikoene som gjelder utilsiktet eller ulovlig tap, uautorisert bekjentgjøring av eller tilgang til persondata som overføres, lagres eller behandles på andre måter. Det har ingen betydning om en uautorisert bekjentgjøring av data finner sted på grunn av at en hacker setter inn et sofistikert nettbasert angrep på et selskaps nettside, eller fordi en fremmed tar bilder av svært sensitive data som vises på skjermen til en medarbeiders bærbare datamaskin. Begge representerer en like alvorlig risiko og trenger egnede forebyggende strategier.

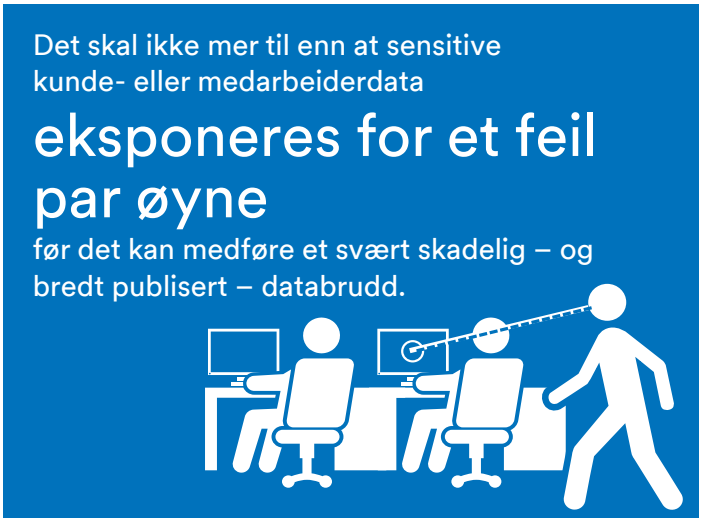
**Sp. Er visuell hacking en risiko?**

**A.** Absolutt.Husk dette: For mange organisasjoner kommer nøklene til ressursene i form av et brukernavn og et passord. Det skal ikke mer til enn et raskt blikk på en ubeskyttet skjerm før en uautorisert person kan få tak i disse nøklene og oppnå tilgang. Risikoen øker også med det økende raffinementet innen sosial manipulering.

For ett år siden ble en journalist hacket mens han arbeidet om bord i et fly.[2] Hackeren kunne beskrive detaljer om en artikkel journalisten holdt på å skrive, personlige e-poster han hadde sendt og kommende jobbmøter – alt sammen informasjon som han sa at han fanget opp ved å hacke flyets Wi-Fi. Eller kanskje det var slik at hackeren ganske enkelt fant informasjonen ved å se på skjermen på journalistens bærbare datamaskin. Journalisten ble rasende, men han forstod meldingen: Mens han arbeidet på en sensitiv artikkel, i dette tilfellet en analyse av de dyptgående og vidtrekkende personvernimplikasjonene av at Apple avviste FBIs forespørsel om dekryptering av telefonen til en terrorist, glemte han å beskytte personvernet og immaterialretten på sin egen enhet. Mange organisasjoner gjør den samme feilen som journalisten og undervurderer risikoen for nettbasert og visuell hacking.

**Sp. Hva er fordelene ved å innføre lavteknologiske, fysiske sikringer?**

**Sv.** Med stadige nyhetsmeldinger om databrudd i stor skala, er det enkelt å glemme at dagens digitale virksomheter fremdeles må forholde seg til fysiske sikkerhetsutfordringer. Det finnes flere fordeler ved å innføre fysiske sikringer, slik som videokamera til overvåkning, låser for vesker til bærbare datamaskiner og personvernfiltre for stasjonære skjermer, bærbare maskiner, nettbrett og smarttelefoner. Personvernfiltre leverer for eksempel en lydbasert strategi til forebygging av personvernkrenkelser og databrudd. Det skal ikke mer til enn at noen sensitive kundedata eller data om medarbeidere vises til feil par øyne før dette kan resultere i potensielt svært skadelige og bredt publiserte databrudd.




De kan også støtte overholdelse av andre regelverk enn GDPR. For noen år siden ble for eksempel en medisinsk assistent ved et sykehus ved Iowa-universitetet oppsagt på grunn av brudd på regler som gjelder vern av personopplysninger om pasienter. Hun ble anklaget for visuell hacking av en medarbeider mens han undersøkte personopplysningene om en pasient i en journal, noe som er en krenkelse av HIPAA.[3]

Fysiske sikringer, slik som personvernfiltre, kan tjene som en visuell påminnelse til medarbeiderne om at anbefalte praksiser for sikkerhet og personvern er noe organisasjonen prioriterer. Og som alltid når det gjelder visuelt personvern, handler det ikke kun om krav til overholdelse. Det handler om å beskytte de mest verdifulle ressursene til en bedrift.

**Sp. Hvordan kan selskaper dra nytte av personvern for å fremme overlegne kundeopplevelser?**

**Sv.**Selskaper som gjennomfører robuste GDPR- og personvernprogrammer opplever en rekke forretningsfordeler utover samsvaret. Å kunne yte en overlegen kundeopplevelse er én av disse. Hvordan organisasjonen din beskytter kundenes data kan ha direkte innvirkning på oppbygging – eller ødeleggelse – av den underliggende opplevelsen av tillit som kundene har til deg.

Vi vet for eksempel at kunder faktisk bytter til konkurrenter som følge av et personvernbrudd.[4] Våre undersøkelser av kunders holdning til personvern understreker videre at 30 prosent av enkeltpersoner avviser å fullføre en nettbasert transaksjon dersom de har lest noe de ikke liker i selskapets personvernmerknad.[5]

Hvis du forplikter deg til å beskytte dataene til kundene dine, og medarbeiderne dine erkjenner og reflekterer denne forpliktelsen i sin samhandling med kundene, kan dette skille deg ut fra konkurrentene.

**Sp. Er det mange selskaper som skiller seg ut på grunn av sin holdning til personvern og sikkerhet?**

**Sv.** Personvern har endret seg fra å være et nisjeemne for juridiske avdelinger til en kjerneverdi for mange organisasjoner. I dag er IT- og markedsføringslederne blant de lederne som mener at beskyttelse av dataressurser fra angrep og misbruk hører til deres øverste prioriteringer. Undersøkelsene våre har vist at 23 prosent av Fortune 100-selskapene har tatt til seg personvern som en del av sitt samfunnsansvar (CSR).[6] Omtrent 70 prosent inkluderte sikkerhet i CSR-rapportene sine.

23 % av Fortune 100-selskapene har innført personvern som en del av sitt samfunnsansvar (CSR).

Vi har også registrert at bedrifter som forplikter seg til personvern og sikkerhet drar fordel ved å være åpne og gjennomsiktige om hvordan de håndterer personopplysninger. Dette kan være en svært verdifull måte å betrygge både kunder, medarbeidere og forretningspartnere på. Det er imidlertid ikke enkelt å drive i samsvar med denne forpliktelsen. Mange ganger må organisasjonene endre hvordan de driver for å innføre disse forpliktelsene i praksis og etablere en bedriftskultur som anerkjenner personvern og sikkerhet som kjerneverdier.

**Sp. Er lignende regelverk som GDPR på vei?**

**A.** Uten tvil:GDPR signaliserer en trend. Vi har nylig fullført en ny undersøkelse som analyserer personvernreglene og -praksisene i 54 land.[7] Det er klart at regioner som Asia og Stillehavsområdet ser på GDPR som en mulig utvikling av lokale personvernregler. Elementer av GDPR, som f.eks. hvor data oppbevares, bygges også inn i databeskyttelsesregler i Latin-Amerika og Russland. Endelig arbeider Europaparlamentet for øyeblikket med å oppdatere kravene til det gjeldende direktivet for elektronisk personvern (ePrivacy Directive). Det gjenstår fremdeles utforming av detaljer, men planen er å innrette elektroniske personvernkrav i samsvar med GDPR.



[1]Forrester Business Technographics Security Survey, 2017
[2]Digital Trends, «Apple vs FBI shown in different light as journalist hacked mid-flight», 25. januar 2016
[3]Veriphyr, «Medical Assistant Fired for "Shoulder Surfing" and Breaching Patient Data Privacy», 2011
[4]Ponemon Institute, «The Impact of Data Breaches on Reputation and Share Value», mai 2017
[5]Forrester Research Consumer Technographics European Online Benchmark Survey (del 2), 2016
[6]Forrester-rapport «The Future of Data Security and Privacy: Growth And Competitive Differentiation», 2017
[7]Forrester «Interactive Data Privacy Heat Map», 2017

FORRESTER®