Fysisk sikkerhet og personvernsikring i henhold til GDPR

EUs generelle personvernforordning (GDPR – European Union General Data Protection Regulation) krever at organisasjoner verden over tenker nytt om hvordan de får tilgang til, bruker og opprettholder personopplysninger. Denne rapporten beskriver scenarier for datarisikoer som kan resultere i administrativ inngripen og økonomiske straffer under det nye regelverket. Den utforsker også anbefalte praksiser for fysisk sikkerhet og personvern – da disse representerer et viktig, men ofte oversett område innen databeskyttelse. Sammen kan administrative, nettbaserte og fysiske sikringer bidra til å beskytte sensitive personopplysninger og vise en organisasjons forpliktelse til personvern.

Viktigste lærdom:

- Lær hva GDPR sier om fysisk sikkerhet og personverntiltak for å beskytte personopplysninger.
- Undersøk hva bransjeeksperter anser for å være et rimelig nivå av databeskyttelse og personvern.

Livet i en datadrevet verden
I disse dager samler de fleste organisasjoner inn og bruker personopplysninger som en naturlig del av sin forretningsvirksomhet – enten om personalet, kunder, mulige kunder eller tredjeparter. Disse dataene oppbevares vanligvis i elektronisk form der det er enkelt for organisasjonen og eksterne parter å få tilgang til dem[1]. I tillegg er hovedfunksjonen til enkelte organisasjoner å samle inn og analysere volumer av personopplysninger.

Selv om mengden og typen data som hver organisasjon samler inn varierer, er det bred enighet om at det aldri har vært enklere å finne dem. Enkeltpersoner etterlater seg omfattende dataspor når de oppretter profiler på sosiale medier, deltar i nettsamfunn, gjennomfører søk på internett, svarer på spørreundersøkelser og drar fordel av salgsfremmende tilbud og «gratis» tjenester, så som lagring av bilder og strømming av musikk.

Teknologien støtter videre prosessen med å bygge robuste profiler på mennesker, med fremskritt innen kunstig intelligens, e-tagger, usynlige sporingsbilder, informasjonskapsler og andre overvåkningsverktøy.

Samlet har innsatsen innen teknologi og datautvinning gjort det mulig for organisasjoner å samle seg et forråd med personopplysninger. Disse reservoarene kan avsløre en persons alder, sivilstand, fødselsdato, utdanning, hobbyer, religion, arbeidshistorikk, politiske meninger, kjøpspreferanser, foretrukne nyhetskilder, inntekt, rulleblad og mye, mye mer.

Selv om mye av disse dataene er sentralisert i selskapenes databaser, finnes det ofte spredte lommer av data gjennom forsyningskjeden i adskilte systemer – ofte uten noen mekanisme for å formidle til fremtidige mottagere av disse dataene hvordan eller hvorfor de ble samlet inn. Dette utsetter personopplysninger for bruk som ligger langt utenfor det formålet de opprinnelig ble innhentet for.

På en hvilken som helst dag kan en lang rekke mennesker innenfor en organisasjon få tilgang til de lagrede dataene – for eksempel for å betale en medarbeider, gjennomføre en markedsundersøkelse, lansere en e-postbasert markedsføringskampanje eller spore en kundes engasjement. Hvert tilgangspunkt til disse dataene representerer en mulighet for at persondata kan bli misbrukt eller falle i feil hender.

Hurtigfakta

Hva er GDPR?
EUs generelle personvernforordning (GDPR – General Data Protection Regulation) har til hensikt å beskytte personvernet for enkeltpersoner i Den europeiske union (EU).

Når trer den i kraft?
25. mai 2018

Hvem gjelder den for?
Alle bedrifter – uansett geografisk sted – som kontrollerer eller behandler personopplysninger for datasubjekter i Den europeiske union.

Hva utgjør personopplysninger?
Enhver opplysning som er forbundet med en faktisk person eller et datasubjekt. Det kan være alt fra et navn, et bilde, en e-postadresse, bankopplysninger, innlegg på nettsider for sosiale medier, medisinske opplysninger eller IP-adressen til en datamaskin.

Hva er effekten?
En bot på EUR 20 millioner eller opptil 4 % av årlig global omsetning (alt etter hva som er høyest). Dette er den maksimale boten som kan ilegges for de mest alvorlige krenkelsene.

Hvor kan jeg henvende meg for mer informasjon?

- En oversikt over regelverket
- Les regelverket
- Fysiske sikkerhetsløsninger

65 %
av respondentene sa at databruddhendelser fikk dem til å miste tilliten til organisasjonen som opplevde det.[5]

Tenk gjennom følgende scenarier for å forstå de fysiske sikkerhetsrisikoene som organisasjoner står overfor:

En medarbeider går gjennom sensitive data på telefonen sin mens vedkommende er på en flyplass, og legger ikke merke til at en person som står i nærheten ser på skjermen hans.

- En medarbeider mister den bærbare datamaskinen sin og informasjonen på enheten er ikke kryptert.
- En medarbeider går vekk fra pulten sin for å fylle på kaffekoppen og har etterlatt kontaktinformasjon for kunder synlig på skjermen eller pulten da en uautorisert iakttaker går forbi.
- En misfornøyd medarbeider tar bilder av dokumenter som har blitt liggende igjen på en skriver, informasjon som vises på en skjerm og påloggingslegitimasjon som er klistret på skjermen til en datamaskin.
- Foreldede bærbare eller stasjonære datamaskiner doneres til et veldedig formål uten at harddiskene er fullstendig slettet.
- Et legekontor avslutter sin virksomhet og kaster pasientjournaler i søppelet uten å makulere dem først.

I 2016 brøt hackere seg inn i
1 milliard registre[2]

Scenarier som disse er i økende grad bekymringsverdige, da databrudd er blitt alt for vanlig i dagens digitaliserte verden. Forrester rapporterer at i 2016 brøt hackere seg inn i én milliard dataregistre på bare 12 måneder. I første halvdel av 2017 ble det rapportert at 918 databrudd ledet til kompromittering av 1,9 milliarder dataregistre globalt. Dette representerer en økning på 164 prosent sammenlignet med de seks første månedene av 2016.[2]

Med hvert nye databrudd øker uroligheten for at databeskyttelse generelt går tapt. Ifølge en nyere studie opplever folk at personvernet deres utfordres av sikkerhets- og konfidensialitetsproblemer. Det er faktisk slik at 91 prosent frykter at enkeltpersoner har mistet kontrollen over hvordan personopplysningene deres samles inn og brukes av bedrifter. Nesten like mange tror det vil være svært vanskelig å fjerne unøyaktig informasjon om dem selv på Internett.[3] Det er ikke bare store innbrudd de bekymrer seg om. Små bedrifter kan ha mindre informasjon om en enkeltperson, men den er ikke mindre viktig for disse enkeltpersonene om den går tapt eller stjeles.

Denne frykten fortsetter å bygge seg opp, selv om strenge personvern- og databeskyttelsesdirektiver og -regelverk har vært i kraft i mer enn ti år. Den amerikanske loven om helseforsikring og ansvarlighet (Health Insurance Portability and Accountability Act, HIPAA), loven om rettferdig kredittrapportering (Fair Credit Reporting Act) og EUs databeskyttelsesdirektiv er noen få fremtredende eksempler.

Databeskyttelsesdirektivet trekker opp prinsipper, slik som kravet om at data skal være sikre, behandles for begrensede formål og ikke bevares lengre enn nødvendig. Siden dette er et «direktiv» og ikke en lov, varierer imidlertid implementeringen og håndhevelsen i hvert land i Europa.

Her kommer GDPR inn
GDPR er det mest omfattende og globalt betydningsfulle regelverket innført for å beskytte personopplysninger. Det ble utformet som følge av en felles oppfatning av at alle har en fundamental rett til personvern. Det har som mål å beskytte personvernet for enkeltpersoner i EU ved å håndheve regelverket for hvordan bedrifter beskytter, behandler og bruker personopplysninger.

GDPR kan være det viktigste fremskrittet innen reguleringen av datasikkerhet og personvern på 20 år – både på grunn av kravene til ansvarlighet når det gjelder registerføring og dets potensielle økonomiske innvirkning. Med to nivåer på bøter kan organisasjoner straffes med 2 prosent av årlig global omsetning/EUR 10 mill. for krenkelser, slik som:

- Manglende melding til tilsynsmyndigheter og berørte enkeltpersoner om et databrudd
- Manglende oppnevning av en databeskyttelsesansvarlig (DPO) hvis organisasjonen krever én

Organisasjoner kan ilegges en bot på 4 prosent av årlig global omsetning/EUR 20 millioner for krenkelser, slik som:

- Manglende overholdelse av et datasubjekts rettigheter
- Manglende overholdelse av et pålegg fra en tilsynsmyndighet
- Manglende overholdelse av krav til internasjonale dataoverføringer[4]

Disse bøtene kommer i tillegg til tap av omdømme, varemerkeverdi og -tillit – noe som kan være like ødeleggende for sluttresultatet til et selskap. Det forholder seg faktisk slik at databruddhendelser sies å ha medført at 65 prosent av enkeltpersoner mister tilliten til organisasjonene som opplever dem.[5]

GDPR-samsvar er ingen liten sak, da det stiller organisasjoner til ansvar for hvordan de samler inn, bruker, bevarer og fjerner personopplysninger, samtidig som de holder dem sikre. Selv de som allerede har personvern- og sikkerhetsprogrammer på plass, må evaluere prosessene sine på nytt. GDPR krever

GDPR er det mest omfattende og globalt mest betydningsfulle regelverket innført for å beskytte personopplysninger.[1]

spesifikt at organisasjoner innfører egnede tekniske og organisasjonsmessige tiltak for å hindre tap av eller uautorisert tilgang til personopplysninger.

Dette har fått mange til å stille spørsmål som:

Sp. Hva representerer personopplysninger?
Sv. Enhver opplysning forbundet med en identifisert eller identifiserbar naturlig person.[6] Dette kan omfatte identifikatorer (som f.eks. et navn eller et ID-nummer) eller opplysninger som avslører rasemessig eller etnisk opprinnelse, politiske oppfatninger, religiøs eller filosofisk overbevisning, fagforeningsmedlemskap, genetiske data, helseopplysninger, straffedommer, prognoser om ytelse på jobben, økonomisk situasjon, personlige preferanser eller interesser, pålitelighet eller adferd, oppholdssted eller bevegelser osv.[7]

Sp. Hva er pseudonymisering, og hvorfor bør jeg bry meg om det?
Sv. Begrepet «pseudonymisering» nevnes 15 ganger i GDPR – en prosedyre som identifiserer felt der en dataoppføring erstattes av én eller flere kunstige identifikatorer eller pseudonymer. GDPR anbefaler at man benytter pseudonymisering på personopplysninger for å redusere risikoene for datasubjekter og hjelpe kontrollører og behandlere til å innfri sine forpliktelser angående databeskyttelse.[8]

Sp. Kan organisasjoner få samtykke fra enkeltpersoner til å samle inn deres personopplysninger?
Sv. Ja, men samtykket må gis ved en tydelig, bekreftende handling som etablerer en fritt avgitt, spesifikk, informert og utvetydig indikasjon på at datasubjektet samtykker i behandlingen av personopplysningene. Forhåndsmerkede bokser, taushet og inaktivitet utgjør ikke samtykke.[9] Organisasjoner må opprettholde et register over å ha mottatt samtykke, og må sikre at samtykkeforespørsler kan skilles fra andre forespørsler ved bruk av et tydelig og enkelt språk.[10] Artikkel 13 trekker opp omfattende informasjon som må oppgis til datasubjektet på det tidspunktet da personopplysninger samles inn, slik som formålet med innhenting av opplysningene, mottagerne eller kategoriene av mottagere av personopplysningene og tidsperioden for oppbevaring av dataene.

Sp. Hva er Data Protection Impact Assessment (DPIA) – konsekvensanalyse av databeskyttelse?
Sv. En DPIA, som er påkrevd for høyrisiko-aktiviteter, hjelper organisasjoner med å evaluere opprinnelsen til, karakteren av, særegenheten og alvorligheten ved risikoer og implementere egnede tiltak for å imøtegå risikoene, slik som kryptering. Ved vurdering av datasikkerhetsrisikoer må det tas hensyn til risikoene som representeres ved behandling av personopplysninger, så som tilfeldig eller ulovlig destruering, tap, endring, uautorisert bekjentgjøring av, eller tilgang til personopplysninger som overføres, lagres eller behandles på annen måte som kan lede til fysisk, materiell eller ikke-materiell skade.[11]

Sp. Må jeg utnevne en databeskyttelsesansvarlig (DPO)?
Sv. Utnevnelse av en DPO er obligatorisk i alle tilfeller der databehandling utføres av en offentlig myndighet (unntatt av domstoler som handler i sin juridiske kapasitet), eller for et selskap hvis kjernevirksomhet består i behandlingsoperasjoner som krever regelmessig og systematisk overvåkning av datasubjekter i stor skala. En DPO er også obligatorisk for alle virksomheter som i stor skala behandler data som omhandler sensitive opplysninger, slik som helse og religiøs eller politisk overbevisning. Spesifikt for DPO-en er at vedkommende:

- Må utnevnes på grunnlag av faglig dyktighet og i særdeleshet ekspertise innenfor databeskyttelseslover og -praksiser
- Kan være en ansatt eller en ekstern tjenesteleverandør
- Det må oppgis kontaktopplysninger for den relevante DPA-en
- Må utstyres med egnede ressurser til å gjennomføre oppgavene sine og opprettholde fagkunnskapen sin
- Må rapportere direkte til den øverste ledelsen
- Må ikke utføre noen andre oppgaver som kan medføre interessekonflikter.[12]

Krav til fysisk sikkerhet og personvern
Hva bør organisasjoner gjøre for å hindre databrudd? Artikkel 24 i GDPR skisserer en organisasjons ansvar for å implementere «egnede tekniske og organisatoriske tiltak» for å sikre og demonstrere riktig behandling av personopplysninger. Artikkel 32 går et steg videre og forklarer at «Ved vurdering av egnet sikkerhetsnivå skal det tas hensyn til risikoene som representeres av behandling, særlig fra utilsiktet eller ulovlig destruering, tap, endring, uautorisert bekjentgjøring av eller tilgang til personopplysninger som overføres, lagres eller behandles på annen måte».

En viktig side ved dette regelverket er vekten det legges på å hindre uautorisert tilgang. Her er fysisk sikkerhet grunnleggende. Den kan spesifikt bidra til å sikre data mot interne og eksterne trusler fra fysiske personer som har til hensikt å utnytte mangler i organisasjonens beskyttelse og gjennom arbeidsstyrken din. Dette inkluderer begrensning av hvilke data som kan observeres, stjeles eller skaffes tilgang til. Gå gjennom følgende og vurder om arbeidsstyrken din har egnede tekniske og organisatoriske tiltak på plass for å være i samsvar.

Implementer innebygd databeskyttelse som standard i designet:
For å beskytte data som standard, må organisasjoner forebyggende identifisere og kun samle inn personopplysninger som er nødvendige for det tiltenkte formålet, kun bevare dataene så lenge som nødvendig (minimeringsprinsippet) og sikre at personopplysninger ikke er tilgjengelige for et ubegrenset antall mennesker. Dette vil sannsynligvis involvere å sikre at personvernrisikoer identifiseres på forhånd og at systemer designes for å imøtegå disse risikoene, relevant pseudonymisering og anonymisering, innføre transparens innenfor behandlingsfunksjonene og identifisere bestemte personer eller roller som trenger tilgang til dataene. Spør deg selv: Tar du hensyn til personvernrisikoer for enkeltpersoner før du designer informasjonssystemene, forretningspraksisene og det fysiske designet? Har du hatt møte med IT-staben din for å gå gjennom nåværende systemer og behandlingsaktiviteter og drøfte om ytterligere trinn er nødvendig for å dokumentere hvordan personopplysninger vil bli beskyttet gjennom hele livssyklusen for informasjonen?

Bruk av fysiske sikringer:
Selv om elektroniske sikkerhetskontroller, slik som datakryptering og komplekse passord, er avgjørende, er «lavtekniske» administrative og fysiske kontroller like viktige. For å fastsette hvor det er behov for fysiske barrierer, må du identifisere hvor det fås tilgang til sensitiv informasjon. Medarbeidere bruker for eksempel ofte mobilenhetene sine for å få tilgang til og dele data fra hvor som helst. Et økende antall av disse medarbeiderne åpner sensitiv informasjon på offentlige steder, ofte med fullt innsyn fra andre. Det er også økt risiko for dataeksponering innenfor kontoret. De vanlige åpne kontorlandskapene fjerner fysiske barrierer som tradisjonelt hjalp til å skjerme datamaskinskjermer. Spør deg selv: Har du plassert datamaskinskjermer vekk fra vinduer, dører og områder som er offentlig tilgjengelige? Utstyrer du stasjonære skjermer og mobile enheter med personvernskjermer for å skjerme mot visning av informasjon for potensielle iakttakere? Befinner delte skrivere/kopimaskiner/telefakser seg i beskyttede områder, eller har de deksler som kan låses? Oppbevarer du fysiske kopier av data i adgangsregulerte anlegg? Utstedes det som standard makuleringsmaskiner til alle lokale enheter, særlig ved kopimaskiner, skrivere og telefakser, og som en forutsetning for alle som bruker telekommunikasjon eller eksterne tilkoblinger for å få tilgang til selskapets informasjonsressurser?

Planlegge opplæring av medarbeidere:
Opplæringsprogrammer skal dekke tre nøkkelaspekter: Anbefalte praksiser for observasjon, fysisk tilgang og forhindring av tyveri. Medarbeidere må for eksempel minnes på å være oppmerksomme på omgivelsene sine når de skaffer tilgang til og bruker tilkoblede enheter fra offentlige steder via bærbare datamaskiner, nettbrett og smarttelefoner. Skjermen på enheten må ikke eksponeres for forbipasserende og potensielle iakttakere, særlig når man angir påloggingsinformasjon eller viser sensitive kontodetaljer. Når det gjelder fysisk tilgang, må organisasjoner lære opp medarbeiderne til å fjerne informasjon fra tavler og samle inn konfidensielle papirer etter møter, lære seg å huske passord i stedet for å skrive dem ned, låse arkivskap og bærbare datamaskiner, bruke personvernfiltre på databehandlingsutstyr og opprettholde en policy for et ryddig skrivebord, inkludert avlogging fra enheter som er uten tilsyn. Spør deg selv: Omfatter opplæringsprogrammene dine situasjonsbestemt bevissthet slik at medarbeiderne kan lære å være oppmerksomme på omgivelsene og kan identifisere og reagere på mistenkelig adferd? Forstår medarbeiderne i organisasjonen forventningene når det gjelder retningslinjene for «ryddig skrivebord»? Minner du medarbeiderne ofte om gode sikkerhetspraksiser som de må følge?

Utarbeide tydelige retningslinjer:
For å vise en organisasjons forpliktelse til innføring av egnede sikkerhets- og personverntiltak må retningslinjene beskrive «skal» og «skal ikke» når det gjelder medarbeidernes og kontraktørenes visning og bruk av informasjon på arbeidsplassen og når de arbeider eksternt. Medarbeideravtaler må inneholde spesifikke formuleringer om ansvaret for å sikre sensitiv og konfidensiell informasjon.[13] Spør deg selv: Har du formidlet personvern- og sikkerhetspraksiserklæringene til enkeltpersoner og forklart hvordan organisasjonen beskytter, deler, avhender og gir tilgang til personopplysninger? Har du retningslinjer for bruk av personlige enheter (BYOD-retningslinjer) som styrer medarbeidernes adferd og påkrevde sikkerhetskontroller når de skaffer tilgang til selskapets ressurser fra de personlige enhetene sine? Krever du, som ledd i sikkerhetsretningslinjene, at medarbeiderne bruker både visuelle og elektroniske sikkerhetskontroller?

Sette grenser for datalagring:
Fastsett tidsperioder for hvor lenge personopplysninger oppbevares – i samsvar med gjeldende lover. Foreta sikker sletting av alle personopplysninger som ikke er absolutt nødvendig for å støtte de forretningsformålene de ble samlet inn for. Spør deg selv: Hvilke tekniske kontroller har du på plass slik at data fjernes til riktig tid? Innfrir destrueringsprosessene i organisasjonen de strenge sikkerhetsretningslinjene, slik som oppgitt av NIST spesialpublikasjon 800–88, f.eks. destruering av harddisker som skal avhendes?

Bekreft tredjepartsleverandører:
Bruk kun prosessorer som gir tilstrekkelig garanti med hensyn til fagkunnskap, pålitelighet og ressurser til å implementere tekniske og organisatoriske tiltak, inkludert behandlingssikkerhet. Spør deg selv: Har du på plass et leverandørprogram som inkluderer kontraktsfestede forpliktelser og etablerer administrative oppsynsaktiviteter for tredjeparter med tilgang til personopplysninger?

Opprett en databruddsprotokoll:
Organisasjoner må være forberedt på å varsle tilsynsmyndighetene uten forsinkelse når de blir oppmerksomme på at det har forekommet brudd på personopplysninger (så snart det lar seg gjøre og ikke senere enn 72 timer). Eller, de må kunne vise at innbruddet i persondataene sannsynligvis ikke vil resultere i en risiko for rettighetene og frihetene til faktiske personer. Hvis det foreligger en høy risiko, må datasubjektene også varsles om databruddet, uten unødvendig forsinkelse.[14] Spør deg selv: Når gikk du sist gjennom organisasjonens hendelsesrespons og retningslinjer og planer for varsling om databrudd? Vet medarbeiderne hvem innenfor organisasjonen de skal varsle dersom enheten deres kompromitteres eller de blir oppmerksomme på et databrudd? Har du på plass en oppdatert plan for hendelsesrespons og varsling av brudd som fastsetter når og hvordan man varsler myndighetene om et databrudd?

Kjenn den enkeltes rettigheter:
EU-borgere har nå rett til å se hvilke personopplysninger organisasjoner har om dem – og under bestemte omstendigheter be om at opplysningene slettes. Retten til sletting krever at organisasjoner sletter enhver kobling til eller kopier eller reproduksjoner av disse personopplysningene. Organisasjoner må sørge for at det finnes en fremgangsmåte for å foreta forespørsler elektronisk, særlig hvis personopplysningene behandles via elektroniske midler.[15] Spør deg selv: Forstår organisasjonen din hva som ansees som «personopplysninger» og hvordan man besvarer henvendelser som gjelder personopplysninger?

Konklusjon:

GDPR er den viktigste endringen innenfor personvernregler på 20 år. Forordningen krever at personopplysninger administreres på en måte som hjelper til å sikre egnet sikkerhet og konfidensialitet – en oppgave som krever både tekniske og organisatoriske sikkerhetstiltak. Og bøtene for manglende overholdelse kan være lammende. De anbefalte praksisene som skisseres i regelverket er imidlertid ganske enkelt god forretningsskikk. Ingen enkeltpersoner ønsker at informasjonen deres misbrukes, og ingen organisasjon ønsker å stå overfor følgene av et databrudd. Organisasjoner som ikke ser personvern som en samsvarsbyrde, men som et selskapsansvar, kan benytte dette som en strategisk fordel for å forbedre omdømmet og merkevareverdien, tiltrekke seg bedre medarbeidere og til syvende og sist opprettholde offentlighetens tillit.

3mnorge.no/3M/no_NO/privacy-protection-ndc/visual-privacy-issues/data-security-study

[1]Forrester, Lessons Learned from the World's Biggest Security Breaches and Data Abuses, 9. januar 2017
[2]2017 Gemalto Breach Level Index, http://www.gemalto.com/press/Pages/First-Half-2017-Breach-Level-Index-Report-Identity-Theft-and-Poor-Internal-Security-Practices-Take-a-Toll.aspx
[3]GfK Privacy Panel, Public Perceptions of Privacy and Security in the Post-Snowden Era, 2014.
[4]Artikkel 83, GDPR, 2017
[5]Ponemon Institute, The Impact of Data Breaches on Reputation & Shared Value, sponset av Centrify, 2017.
[6]Artikkel 4, GDPR, 2017
[7]Foredrag 75, GDPR, 2017
[8]Foredrag 26 og 28, GDPR, 2017
[9]Foredrag 32, GDPR, 2017
[10]Artikkel 7, GDPR, 2017
[11]Artikkel 35 og foredrag 83–84, GDPR, 2017
[12]Artikkel 37–38, GDPR, 2017
[13]Foredrag 74, 77–78, GDPR, 2017
[14]Foredrag 81, GDPR, 2017
[15]Foredrag 59, 63, 65, 66, GDPR, 2017