GDPR – Fysiske sikkerhedsforanstaltninger vedrørende beskyttelselse af privatlivets fred

Den Europæiske Unions generelle forordning om databeskyttelse (GDPR) kræver, at organisationer over hele verden skal genoverveje, hvordan de får adgang til, bruger og vedligeholder personoplysninger. Denne hvidbog beskriver datariskoscenarier, der kan resultere i administrativ indgriben og økonomiske sanktioner i henhold til den nye forordning. Den undersøger også bedste praksis for fysisk sikkerhed og beskyttelse af privatlivets fred – da disse procedurer repræsenterer et vigtigt men ofte overset område inden for databeskyttelse. Sammen kan administrative, cyber og fysiske sikkerhedsforanstaltninger bidrage til at beskytte følsomme personoplysninger og påvise en organisations forpligtelse med hensyn til databeskyttelse.

Vigtigste budskaber:

- Lær, hvad Databeskyttelsesforordningen har at sige om fysiske sikkerhedsforanstaltninger vedrørende beskyttelse af personoplysninger og privatlivets fred.
- Udforsk, hvad brancheeksperter anser som værende et rimeligt niveau for databeskyttelse og beskyttelse af privatlivets fred.

Vi lever i en verden, der er drevet af data
Som en naturlig del af at drive forretning i dag indsamler og bruger de fleste organisationer personoplysninger – hvad enten det er om personale, kunder, kundeemner eller tredjeparter. Disse oplysninger gemmes typisk i elektronisk form, hvor organisationen[1] og eksterne parter kan få adgang til dem. Endvidere er nogle af organisationernes hovedformål at indsamle og analysere mængder af personoplysninger.

Mens mængden og typen af oplysningerne, som indsamles af hver enkelt organisation, varierer, er der bred enighed om, at det aldrig har været nemmere at finde dem. Mennesker efterlader sig en stribe af oplysninger, når de opretter profiler på sociale medier, deltager i onlinefællesskaber, søger på internettet, besvarer undersøgelser og drager fordel af kampagner og "gratis" tjenester, som fx til billedopbevaring og streaming af musik.

Teknologi hjælper processen med at opbygge robuste profiler om personer yderligere gennem fremskridt inden for kunstig intelligens, e-tags, web-beacons, cookies og andre overvågningsværktøjer.

Sammen har teknologi- og dataudvindingsindsatsen gjort det muligt for organisationer at indsamle enorme mængder personoplysninger. Disse datadepoter kan afsløre en persons alder, civilstand, fødselsdag, uddannelse, hobbyer, religion, beskæftigelseshistorik, politiske overbevisninger, købspræferencer, foretrukne nyhedskilder, indkomst, kriminel baggrund og meget mere.

Selvom mange af disse oplysninger er centraliseret i virksomhedsdatabaser, er datalommer ofte spredt over forsyningskæden i uensartede systemer, og der mangler ofte mekanismer til at informere de fremtidige modtagere af oplysningerne, hvordan eller hvorfor de oprindeligt blev indsamlet. Dette udsætter personoplysninger for anvendelser langt væk fra det formål, som de oprindeligt blev indsamlet til.

På en given dag kan mange personer i en organisation få adgang til de lagrede data – måske for at betale en medarbejder, foretage markedsundersøgelser, lancere en e-mailmarketingkampagne eller spore customer engagement. Hvert adgangspunkt til disse datapuljer udgør en mulighed for, at personoplysningerne misbruges eller falder i de forkerte hænder.

Hurtige fakta

Hvad er GDPR?
Den generelle forordning om databeskyttelse (GDPR) sigter mod beskyttelse af privatlivets fred for personer i Den Europæiske Union (EU).

Hvornår træder den i kraft?
25. maj 2018

Hvem påvirker den?
Alle virksomheder – uanset placering – der kontrollerer eller behandler personoplysninger om registrerede personer i Den Europæiske Union.

Hvad udgør personoplysninger?
Enhver form for information om en fysisk person eller en registreret borger. Det kan være alt fra et navn, et foto, en e-mailadresse, bankoplysninger, indlæg på sociale netværk, medicinske oplysninger eller en computers IP-adresse.

Hvilken indvirkning får forordningen?
En bøde på 20 mio. EUR eller op til 4 % af den globale årlige omsætning (såfremt dette beløb er højere). Dette er den maksimale bøde, der kan pålægges for de mest alvorlige overtrædelser.

Hvor kan jeg finde flere oplysninger?

- En oversigt over forordningen
- Læs forordningen
- Fysiske sikkerhedsløsninger

65 %
af respondenterne siger,
at brud på datasikkerheden fik dem til at miste tilliden til den organisation, der oplevede bruddet.[5]

For at forstå de fysiske sikkerhedsrisici, som organisationer står overfor, skal du overveje disse scenarier:

En medarbejder gennemgår følsomme oplysninger på sin telefon i lufthavnen og bemærker ikke, at nogen i nærheden kigger på skærmen.

- En medarbejder mister sin bærbare computer, og oplysningerne på harddisken er ikke krypterede.
- En medarbejder forlader sit skrivebord for at hente en kop kaffe, mens kundekontaktoplysninger vises på skærmen eller skrivebordet, da en uvedkommende går forbi.
- En utilfreds medarbejder tager billeder af dokumenter, der er efterladt i en printer, oplysninger, der vises på en skærm, og login-oplysninger, der er tapet til en computerskærm.
- Forældede bærbare eller stationære computere doneres til velgørenhed, uden at harddiskene slettes helt.
- Et lægekontor lukker og smider patientjournaler i skraldespanden uden at makulere dem.

Det er scenarier som disse, der bliver mere og mere foruroligende, da brud på datasikkerheden er alt for almindelige

I 2016 kompromitterede hackere
1 mia. fortegnelser[2]

i nutidens digitaliserede verden. Forrester rapporterer, at hackere i 2016 kompromitterede over én milliard optegnelser i løbet af bare 12 måneder. I første halvdel af 2017 blev det rapporteret, at 918 brud på datasikkerheden medførte, at 1,9 milliarder dataoptegnelser blev kompromitteret på verdensplan. Dette er en stigning på 164 % i forhold til de første seks måneder af 2016.[2]

Med hver nyt brud på datasikkerheden er der voksende bekymring for, at databeskyttelse snart hører fortiden til. Ifølge en nylig undersøgelse føler folk, at deres privatliv udfordres af problemer med sikkerheden og fortroligheden. Faktisk frygter 91 %, at vi har mistet kontrollen over, hvordan vores personoplysninger indsamles og anvendes af virksomheder. Næsten lige mange mener, at det ville være yderst svært at fjerne unøjagtige oplysninger om sig selv online.[3] Det er ikke kun store overtrædelser, der er et problem. Små virksomheder kan ligge inde med færre oplysninger om en person, men det er ikke mindre vigtigt for de pågældende personer, hvis disse oplysninger stjæles eller misbruges.

Denne frygt fortsætter med at stige, selvom strenge databeskyttelsesdirektiver og -bestemmelser har eksisteret i mere end et årti. HIPAA (Health Insurance Portability and Accountability Act), Fair Credit Reporting Act og EU's databeskyttelsesdirektiv er et par typiske eksempler.

Databeskyttelsesdirektivet skitserer principper, såsom kravet om, at data skal sikres, behandles til begrænsede formål og ikke opbevares længere end nødvendigt. Men som et "direktiv" snarere end en lov varierede implementeringen og håndhævelsen i de enkelte lande i Europa.

Om GDPR
Databeskyttelsesforordningen (GDPR) er den mest omfattende og globalt virkningsfulde forordning, som er blevet introduceret med henblik på beskyttelse af personoplysninger. Den blev oprettet på grund af den fælles tro på, at alle har en grundlæggende ret til at beskytte deres privatliv. Den sigter mod at beskytte menneskers privatliv i EU ved at håndhæve en ny forordning om, hvordan virksomheder beskytter, behandler og anvender personoplysninger.

GDPR er meget vel det vigtigste fremskridt inden for datasikkerhed og beskyttelse af privatlivets fred i 20 år – både på grund af dens krav til ansvarlighed vedrørende registrering samt dens potentielle økonomiske konsekvenser. Med to former for bøder kan organisationer straffes med 2 % af den globale årlige omsætning/10 mio. EUR for overtrædelser, såsom:

- Manglende underrettelse af en tilsynsmyndighed og berørte personer om et brud på datasikkerheden
- Manglende udnævnelse af en databeskyttelsesrådgiver (DPO), hvis organisationen kræver en

Organisationer kan få bøder på 4 % af den samlede globale årlige omsætning/20 mio. EUR for overtrædelser, såsom:

- Manglende overholdelse af den registrerede persons rettigheder
- Manglende overholdelse af en ordre fra en tilsynsmyndighed
- Manglende overholdelse af krav til internationale dataoverførsler[4]

Disse bøder er i tillæg til tab af virksomhedens gode navn og rygte, brandværdi og kundetillid – som kan være lige så ødelæggende for virksomhedens bundlinje. Faktisk får brud på datasikkerheden angiveligt 65 % af respondenterne til at miste tillid til den organisation, der oplever bruddet.[5]

GDPR-overholdelse kræver en stor indsats, da forordningen drager organisationer til ansvar for, hvordan de indsamler, bruger, vedligeholder og sletter personoplysninger, samtidig med at de holder dem sikre. Selv organisationer med eksisterende databeskyttelses- og sikkerhedsprogrammer skal revurdere deres processer. GDPR kræver specifikt, at organisationer skal indføre passende tekniske og organisatoriske foranstaltninger med henblik på at forhindre tab af eller uautoriseret adgang til personoplysninger.

Databeskyttelsesforordningen (GDPR) er den **mest omfattende** og **globalt virkningsfulde** forordning, som er blevet introduceret med henblik på **beskyttelse af personoplysninger.**[1]

Dette har affødt spørgsmål, såsom:

Sp.: Hvad udgør personoplysninger?
Sv.: Enhver form for information om en identificeret eller identificerbar fysisk person.[6] Dette kan omfatte identifikatorer (såsom et navn eller et identifikationsnummer) eller data, der afslører race eller etnisk oprindelse, politisk, religiøs eller filosofisk overbevisning, fagforeningsmæssigt tilhørsforhold, genetiske data, helbredsoplysninger, strafbare handlinger; forudsigelse af indsats på arbejdspladsen, økonomisk situation, personlige præferencer eller interesser, pålidelighed eller adfærd, geografisk position eller bevægelser mv.[7]

Sp.: Hvad er pseudonymisering, og hvorfor skal jeg interessere mig for det?
Sv.: Udtrykket "pseudonymisering" omtales 15 gange i Databeskyttelsesforordningen. Det er en procedure, hvormed identificerende felter inden for en datapost erstattes af en eller flere kunstige identifikatorer eller pseudonymer.GDPR anbefaler, at personoplysninger underlægges pseudonymisering med henblik på at reducere risiciene for registrerede personer samt for at bistå dataansvarlige og databehandlere med at opfylde deres databeskyttelsesforpligtelser.[8]

Sp.: Kan virksomheder få samtykke fra enkeltpersoner til at indsamle deres personoplysninger?
Sv.: Ja, men samtykket skal gives i form af en klar bekræftelse, der indebærer en frivillig, specifik, informeret og utvetydig tilkendegivelse fra den registrerede om, at vedkommende accepterer, at dennes personoplysninger behandles. Forudafkrydsede felter, tavshed og inaktivitet udgør ikke et samtykke.[9] Organisationer skal føre fortegnelser over at have modtaget samtykke og sørge for, at anmodninger om samtykke klart kan skelnes fra andre anmodninger og formuleres på et klart og enkelt sprog.[10] Artikel 13 skitserer omfattende oplysninger, der skal gives til den registrerede person på det tidspunkt, hvor personoplysningerne indsamles, såsom formålet med indsamlingen af oplysningerne, modtagere eller kategorier af modtagere af personoplysningerne og det tidsrum, personoplysningerne vil blive opbevaret.

Sp.: Hvad er en konsekvensanalyse vedrørende databeskyttelse (DPIA)?
Sv.: En konsekvensanalyse vedrørende databeskyttelse, som er nødvendig i forbindelse med højrisiko aktiviteter, hjælper organisationer med at evaluere risici, deres oprindelse, karakter, særegenhed og alvor og iværksætte passende foranstaltninger til at begrænse risiciene, såsom kryptering. Ved vurderingen af datasikkerhedsrisikoen bør der tages hensyn til de risici, som behandling af personoplysninger indebærer, såsom hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet, så detkan føre til fysisk, materiel eller immateriel skade.[11]

Sp.: Skal jeg udpege en databeskyttelsesrådgiver (DPO)?
Svar: Udpegelsen af en DPO er obligatorisk, når databehandlingen udføres af en offentlig myndighed (undtagen domstole, der handler i deres egenskab af domstol) eller for et selskab, hvis kerneaktiviteter består i behandlingsaktiviteter, som kræver regelmæssig og systematisk overvågning af de registrerede i stort omfang. En DPO er også obligatorisk for alle virksomheder, der behandler data vedrørende følsomme oplysninger, såsom helbredsoplysninger, religiøs eller politisk overbevisning i stort omfang. En DPO:

- Skal udpeges på grundlag af sine faglige kvalifikationer, navnlig ekspertise inden for databeskyttelsesret og –praksis
- Kan være en medarbejder eller en ekstern serviceudbyder
- Kontaktoplysninger skal gives til den relevante DPA
- Skal forsynes med passende ressourcer til at udføre sine opgaver og opretholde sin ekspertise
- Skal rapportere direkte til det øverste ledelsesniveau
- Må ikke udføre andre opgaver, der kan medføre en interessekonflikt.[12]

Krav til fysisk sikkerhed og beskyttelse af privatlivets fred
Hvad skal organisationer gøre for at forhindre brud på datasikkerheden? Artikel 24 i Databeskyttelsesforordningen skitserer en organisations ansvar for at gennemføre "passende tekniske og organisatoriske foranstaltninger" for at sikre og påvise korrekt behandling af personoplysninger. Artikel 32 går et skridt videre for at forklare, at "ved vurderingen af, hvilket sikkerhedsniveau der er passende, tages der hensyn til de risici, som behandling udgør, navnlig ved hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet."

Et vigtigt aspekt af denne forordning er vægten på at forhindre uautoriseret adgang. Det er her, hvor fysisk sikkerhed er afgørende. Specielt kan det hjælpe med at beskytte data mod interne og eksterne menneskelige trusler, der sigter mod at udnytte huller inden for organisationen og gennem din arbejdsstyrke. Dette omfatter begrænsning af, hvilke data der kan observeres, stjæles eller opnås adgang til. Gennemgå det følgende, og vurdér, om din arbejdsstyrke har passende tekniske og organisatoriske foranstaltninger til at overholde forordningen.

Implementér databeskyttelse gennem design og databeskyttelse gennem standardindstillinger: For at beskytte data gennem standardindstillinger skal organisationer proaktivt kun identificere og indsamle de personoplysninger, der er nødvendige for deres tilsigtede formål, kun opbevare dataene så længe som nødvendigt (minimeringsprincippet), og de skal sikre, at personoplysninger ikke gøres tilgængelige for et ubegrænset antal personer. Dette vil sandsynligvis involvere at sikre, at privatlivsrisici identificeres omgående, at systemer designes til at afhjælpe disse risici, pseudonymisering og anonymisering efter behov, at skabe gennemsigtighed inden for behandlingsfunktionerne og at identificere specifikke personer eller roller, der har brug for adgang til oplysningerne. Spørg dig selv: Tager du højde for privatlivsrisici for enkeltpersoner, før du designer dine informationssystemer, forretningsmetoder og fysiske designs? Har du talt med dit it-personale for at gennemgå aktuelle systemer og behandlingsaktiviteter og for at drøfte, om der er behov for yderligere handlinger for at påvise, hvordan personoplysninger vil blive beskyttet i hele deres livscyklus?

Brug fysiske sikkerhedsforanstaltninger: Selvom cybersikkerhedskontroller, såsom datakryptering og komplekse adgangskoder, er af afgørende betydning, er "lavteknologiske" administrative og fysiske kontroller lige så vigtige. Med henblik på at afgøre, hvor der er behov for fysiske barrierer, skal du identificere, hvor følsomme oplysninger er tilgængelige. Medarbejdere bruger fx ofte mobile enheder til at få adgang til og dele data fra et hvilket som helst sted. Et stigende antal af disse medarbejdere får adgang til følsomme oplysninger på offentlige steder, så alle kan se det. Der er også øget risiko for dataeksponering på kontoret. Åbne kontormiljøer fjerner de fysiske barrierer, der traditionelt har bidraget til at beskytte computerskærme. Spørg dig selv: Har du placeret computerskærmene væk fra vinduer, døre og områder, som er offentligt tilgængelige? Udstyrer du computer- og mobilskærme med beskyttelsesskærme for at dække visningen af oplysninger for potentielle forbipasserende? Er delte printere/kopimaskiner/faxmaskiner placeret i beskyttede områder eller forsynet med låsedæksler? Opbevarer du fysiske kopier af oplysninger i et adgangskontrolleret anlæg? Er makulatorer som standard opstillet ved alle enheder på arbejdspladsen, især ved kopimaskiner, printere og faxmaskiner, og er de en forudsætning for alle, der arbejder eksternt eller bruger eksterne forbindelser til at få adgang til virksomhedens informationsaktiver?

Planlæg medarbejderuddannelse: Uddannelsesprogrammer skal dække tre hovedområder: Bedste praksis for observation, fysisk adgang og tyveriforebyggelse. Medarbejderne skal fx mindes om at være bevidste om deres omgivelser, når de tilgår og betjener tilsluttede enheder fra offentlige steder via deres bærbare computere, tablets og smartphones. Enhedsskærme må ikke vises til forbipasserende og potentielle tilskuere, især ikke når der indtastes loginoplysninger eller vises følsomme kontooplysninger. Hvad angår fysisk adgang, skal organisationer undervise deres medarbejdere i at slette oplysninger fra tavler og indsamle fortrolige papirer efter møder, huske adgangskoder i stedet for at skrive dem ned, låse arkivskabe og bærbare computere, anvende privatlivsfiltre på computerenheder og opretholde en politik om at holde skrivebordene rene og låse uovervågede enheder. Spørg dig selv: Dækker dit uddannelsesprogram situationsbevidsthed, så medarbejderne lærer at være opmærksomme på deres omgivelser og at identificere og reagere på mistænkelig adfærd? Er medarbejderne i stand til at forstå vores organisations forventninger til vores "princip om det tomme skrivebord"? Påminder du ofte medarbejderne om en god sikkerhedspraksis, som de skal følge?

Udarbejd klare politikker: For at demonstrere en organisations forpligtelse til at gennemføre passende foranstaltninger vedrørende sikkerhed og beskyttelse af privatlivets fred skal deres politikker skitsere råd og advarsler i forbindelse med visning og brug af oplysninger til medarbejdere og entreprenører både på arbejdspladsen og ved eksternt arbejde. Medarbejderaftaler skal indeholde det specifikke ansvar for beskyttelse af følsomme og fortrolige oplysninger.[13] Spørg dig selv: Har du formidlet din erklæring om beskyttelse af privatlivets fred og sikkerhed til dine medarbejdere og forklaret, hvordan din organisation beskytter, deler, bortskaffer og giver adgang til personoplysninger? Har du en BYOD-politik for medarbejderadfærd og påkrævede sikkerhedskontroller i forbindelse med medarbejderes tilgang til virksomhedens ressourcer fra deres personlige enheder? Har du som led i din sikkerhedspolitik brug for, at medarbejdere anvender både visuelle og cybersikkerhedskontroller?

Sæt grænser for datalagring: Fastsæt tidsrum for, hvor længe personoplysningerne opbevares – i overensstemmelse med gældende love. Slet på forsvarlig vis alle personoplysninger, der ikke er absolut nødvendige for at udføre de forretningsformål, som de blev indsamlet til. Spørg dig selv: Hvilke tekniske kontroller har du indført, så oplysningerne slettes rettidigt? Opfylder din organisations destruktionsprocesser stærke sikkerhedsretningslinjer, fx som foreskrevet i NIST Special Publication 800-88, såsom fysisk ødelæggelse af harddiske, der har nået slutningen af deres levetid?

Verificér tredjepartsleverandører:
Brug kun databehandlere, der giver tilstrækkelige garantier i form af ekspertise, pålidelighed og ressourcer for implementering af tekniske og organisatoriske foranstaltninger, herunder med hensyn til behandlingssikkerhed. Spørg dig selv: Har du indført et leverandørstyringsprogram, der omfatter kontraktlige forpligtelser og etablerer tilsynsaktiviteter for tredjeparter, som har adgang til personoplysninger?

Opret en protokol for brud på datasikkerheden:
Organisationer skal være forberedte på at underrette tilsynsmyndigheden uden unødig forsinkelse, efter at de er blevet bekendt med, at der er sket et brud på persondatasikkerheden (om muligt senest efter 72 timer). Ellers skal de være i stand til at påvise, at bruddet på persondatasikkerheden sandsynligvis ikke indebærer risiko for fysiske personers rettigheder eller frihed. Hvis der er stor risiko, skal de(n) registrerede også underrettes om bruddet på datasikkerheden uden unødig forsinkelse.[14] Spørg dig selv: Hvornår har du senest gennemgået din organisations hændelsesrespons- og underretningspolitikker og –planer i tilfælde af sikkerhedsbrud? Ved medarbejderne, hvem i organisationen de skal kontakte, hvis deres enhed kompromitteres, eller hvis de bliver opmærksomme på brud på datasikkerheden? Er der indført en opdateret hændelsesrespons- og underretningsplan med henblik på at afgøre, hvornår og hvordan man skal underrette myndighederne om et brud på datasikkerheden?

Kend menneskers rettigheder:
EU-borgere har nu ret til at få indsigt i, hvilke personoplysninger organisationer opbevarer om dem – og anmode om, at deres oplysninger slettes under visse omstændigheder. Retten til sletning kræver, at organisationerne sletter eventuelle links til eller kopier af disse personoplysninger. Organisationer skal give mulighed for elektroniske anmodninger, navnlig hvis personoplysninger behandles elektronisk.[15] Spørg dig selv: Forstår din organisation, hvad der betragtes som "personoplysninger", og hvordan man besvarer henvendelser vedrørende personoplysninger?

Konklusion:

GDPR er den vigtigste ændring i databeskyttelseslovgivningen i 20 år. Den kræver, at personoplysninger håndteres på en måde, der hjælper med at garantere tilstrækkelig sikkerhed og fortrolighed – en opgave, der kræver både tekniske og organisatoriske sikkerhedsforanstaltninger. Og bøderne for manglende overholdelse kan være sønderknusende. Men den bedste praksis, der er beskrevet i forordningen, er ganske enkelt god forretning. Ingen ønsker, at deres oplysninger misbruges, og ingen organisation ønsker at blive udsat for konsekvenserne af et brud på datasikkerheden. Organisationer, der ikke anser beskyttelse af privatlivets fred som en byrde, men som en del af virksomhedens sociale medansvar, kan bruge det som en strategisk fordel til at forbedre deres omdømme og brandværdi, tiltrække bedre medarbejdere og i sidste ende opretholde offentlighedens tillid.

3mdanmark.dk/3M/da_DK/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]Artikel 83, GDPR, 2017
[5]Ponemon Institute, The Impact of Data Breaches on Reputation & Shared Value, sponsored by Centrify, 2017.
[6]Artikel 4, GDPR, 2017
[7]Punkt 75, GDPR, 2017
[8]Punkt 26 og 28, GDPR, 2017
[9]Punkt 32, GDPR, 2017
[10]Artikel 7, GDPR, 2017
[11]Artikel 35 og punkt 83-84, GDPR, 2017
[12]Artikel 37-38, GDPR, 2017
[13]Punkt 74, 77-78, GDPR, 2017
[14]Punkt 81, GDPR, 2017
[15]Punkt 59, 63, 65, 66, GDPR, 2017

The experts in screen privacy. | 3M