De algemene verordening gegevensbescherming over fysieke bescherming en beveiligingsmaatregelen van de privacy

De algemene verordening gegevensbescherming van de Europese Unie (GDPR) schrijft voor dat organisaties wereldwijd hun toegang, gebruik en onderhoud van persoonlijke gegevens moeten herzien. Dit whitepaper beschrijft situaties met gegevensrisico's die onder de nieuwe voorschriften tot administratieve interventie en geldboetes zouden kunnen leiden. Het kijkt tevens naar de beste praktijken in verband met fysieke beveiliging en privacy – met een vorm van gegevensbescherming die belangrijk is, maar die veel over het hoofd wordt gezien. De combinatie van administratieve beveiligingen en cyberbeveiliging en fysieke beveiligingsmaatregelen kan een betere bescherming bieden van gevoelige persoonlijke gegevens, en de toewijding van het bedrijf aan gegevens-privacy demonstreren.

Belangrijke conclusies:

- Vindt uit wat de algemene verordening gegevensbescherming zegt over fysieke beveiliging en privacy ter beveiliging van persoonlijke gegevens.
- Kijk wat de experts in de industrie een redelijke mate van gegevensbescherming en privacy beschouwen.

Het leven in een door gegevens aangedreven wereld
De meeste bedrijven van nu vergaren en gebruiken als normaal onderdeel van hun bedrijfsvoering persoonlijke gegevens – over personeel, klanten, prospects of derden. Deze gegevens worden typisch in elektronische vorm opgeslagen voor toegang door de organisatie' en externe partijen. Bovendien is het de voornaamste functie van sommige organisaties om grote hoeveelheden persoonlijke gegevens te vergaren en analyseren.

Hoewel de hoeveelheden en soorten gegevens die door elke organisatie worden vergaard varieert, is men het er algemeen over eens dat ze gemakkelijker te vinden zijn dan ooit. Individuen laten een duidelijk spoor aan gegevens achter bij het opzetten van profielen in de sociale media, het deelnemen aan gemeenschappen op internet, het zoeken via internet, het invullen van enquêtes en het profiteren van speciale promoties en 'gratis' diensten, zoals voor de opslag van foto's en het streamen van muziek.

De technologie helpt bij het proces van het samenstellen van robuuste profielen van mensen, met de vooruitgangen in kunstmatige intelligentie, e-tags, webbeacons, cookies en andere bewakingsinstrumenten.

Met de combinatie van technologie en gegevensontginning zijn organisaties in staat om grote hoeveelheden persoonlijke gegevens te vergaren. Deze gegevens omvatten vaak hun leeftijd, echtelijke staat, verjaardag, onderwijs, hobby's, religie, arbeidsverleden, politieke meningen, koopvoorkeuren, geprefereerde nieuwsbronnen, inkomen, criminele achtergrond en nog veel meer.

Terwijl veel van deze gegevens zich in de gegevensbestanden van bedrijven bevinden, zijn onderdelen daarvan over verschillende systemen in de leveringsketen verspreid – vaak zonder enig mechanisme om aan de toekomstige ontvangers van de gegevens te laten weten hoe of waar ze aanvankelijk werden vergaard. Zodoende zijn de persoonlijke gegevens blootgesteld aan toepassingen die het doel waarvoor ze werden vergaard ver te buiten gaan.

Snelle feiten

Wat is de algemene verordening gegevensbescherming (GDPR)?
Het doel van de algemene verordening gegevensbescherming (General Data Protection Regulation; GDPR) is om de privacy van individuen in de Europese Unie (EU) te beschermen.

Wanneer gaat die in?
Op 25 mei 2018

Waar heeft die betrekking op?
Alle bedrijven – ongeacht hun locatie – die persoonlijke gegevens van betrokkenen in de Europese Unie beheren of verwerken.

Wat zijn persoonlijke gegevens?
Alle gegevens in verband met een natuurlijke persoon of betrokkene. Dit kan bijvoorbeeld een naam zijn, een foto, een e-mailadres, bankgegevens, posts op sociale-netwerksites, medische gegevens en het IP-adres van een computer.

Wat zijn de gevolgen ervan?
Een boete van €20 miljoen of maximaal 4% van de jaarlijkse omzet (en wel de grootste daarvan). Dit is de maximale boete die voor de ernstige overtredingen kan worden gegeven.

Waar kan ik terecht voor meer informatie?

- Een overzicht van de verordening
- Lees de verordening
- Fysieke beveiligingsoplossingen

65%
van de ondervraagden zei dat zij door incidenten met data-inbreuk het vertrouwen had verloren in de betreffende organisatie.[5]

De opgeslagen gegevens kunnen op elk moment door talloze mensen in de organisatie worden benaderd – misschien om een werknemer te betalen, voor marktonderzoek, om een marketingcampagne per e-mail te lanceren, of om de interactie met klanten te bekijken. Elk toegangspunt tot deze units met persoonlijke gegevens vormt het gevaar van misbruik ervan of dat ze in de verkeerde handen terechtkomen.

Om de fysieke beveiligingsrisico's te begrijpen waar organisaties mee te maken hebben te begrijpen, kijken we naar twee situaties:

Een werknemer bekijkt op het vliegveld gevoelige gegevens op zijn telefoon en merkt niet dat iemand dichtbij naar zijn scherm kijkt.

- Een werknemer verliest zijn laptop en de informatie op de drive is niet gecodeerd.
- Een werknemer loopt van zijn bureau weg om koffie te halen en laat de contactgegevens van een klant op zijn scherm of bureau achter terwijl een onbevoegde langs loopt.
- Een geïrriteerde werknemer neemt foto's van documenten die op een printer zijn achtergelaten, informatie op een scherm, en inloggegevens die op een computerscherm zijn geplakt.
- Verouderde laptops of desktops worden aan liefdadigheidsinstellingen gegeven zonder dat de harde schijf eerst goed wordt gewist.
- De praktijk van een arts sluit en de gegevens van patiënten komen in de vuilnisbak terecht zonder dat ze worden versnipperd.

In 2016 werden door hackers
1 miljard records aangevallen[2]

Dit is het soort situaties dat steeds zorgwekkender wordt en data-inbreuk komt in de gedigitaliseerde wereld van nu veel voor. Forrester vermeldt dat hackers in 2016 in slechts 2 maanden een miljard records hebben aangetast. In de eerste helft van 2017 werd gerapporteerd dat 918 data-inbreuken wereldwijd hadden geleid tot de aantasting van 1,9 miljard gegevensrecords. Dit is een toename van 164 procent vergeleken met de eerste zes maanden van 2016.[2]

Met elke nieuwe data-inbreuk groeit de angst dat data-privacy vrijwel niet meer bestaat. Volgens een recent onderzoek denken mensen dat hun privacy wordt aangetast door problemen met beveiliging en vertrouwelijkheid. 91 Procent van de mensen zijn in feite bang dat individuen hun controle hebben verloren overhoe hun persoonlijke gegevens door bedrijven worden vergaard en gebruikt. Bijna even veel mensen denken dat het heel moeilijk zou zijn om incorrecte informatie over hen van het internet te verwijderen.[3] Men maakt zich niet alleen zorgen over grootscheepse data-inbreuken. Kleine bedrijven hebben misschien minder informatie over een individu maar het is even belangrijk voor die persoon als die wordt gestolen of misbruikt.

Deze angst blijft groeien, hoewel er al meer dan 10 jaar strenge richtlijnen en voorschriften bestaan in verband met de privacy en bescherming van gegevens. The Health Insurance Portability and Accountability Act (HIPAA), The Fair Credit Reporting Act, en de richtlijn inzake gegevensbescherming van de Europese Unie zijn daar prominente voorbeelden van.

De richtlijn inzake gegevensbescherming stelt bepaalde principes. Zoals de vereiste dat de gegevens veilig worden gehouden, voor beperkte doeleinden worden verwerkt en niet langer dan nodig worden bewaard. Omdat het echter een 'richtlijn' is en geen wet varieert de invoering en handhaving ervan in elk land van Europa.

En nu de algemene verordening gegevensbescherming
De algemene verordening gegevensbescherming is de meest omvattende verordening voor de bescherming van persoonlijke gegevens en met de meeste invloed wereldwijd. Deze werd ingesteld omdat men het er gezamenlijk over eens was dat iedereen een fundamenteel recht heeft op privacy. Het doel is om de privacy van individuen in de EU te beschermen door een nieuwe verordening af te dwingen over de manier waarop bedrijven persoonlijke gegevens beschermen, verwerken en gebruiken.

De algemene verordening gegevensbescherming is misschien de belangrijkste vooruitgang op het gebied van de voorschriften inzake gegevensbescherming en -privacy regelgeving in 20 jaar – zowel als gevolg van de vereisten inzake het bijhouden van records als de mogelijke financiële invloed. Met de twee niveaus van boetes kunnen organisaties boetes krijgen van 2 procent van de jaarlijkse omzet/ €10 miljoen voor overtredingen zoals:

- het niet aan een toezicht houdende autoriteit en de betreffende individuen melden van een data-inbreuk
- het niet aanstellen van een functionaris voor gegevensbescherming (DPO) als de organisatie die nodig heeft

Organisaties kunnen boetes ontvangen van 4 procent van de jaarlijkse omzet/€20 miljoen voor overtredingen zoals:

- het niet voldoen aan de rechten van gegevenssubjects
- het niet uitvoeren van een order van een toezicht houdende autoriteit
- het niet voldoen aan vereisten in verband met de internationale overdracht van gegevens[4]

Naast deze boetes spelen nog het verlies van de reputatie en de waarde van en het vertrouwen in het merk – wat even verwoestend kan zijn voor de winst van het bedrijf. In feite wordt vermeld dat 65 procent van mensen door incidenten met data-inbreuk het vertrouwen in de betreffende organisatie verliezen.[5]

De naleving van de algemene verordening gegevensbescherming is geen kleine zaak omdat organisaties verantwoordelijk worden gesteld voor de manier waarop deze de persoonlijke gegevens op een veilige manier vergaren, gebruiken, onderhouden en verwijderen. Zelfs organisaties die al privacy- en beveiligingsprogramma's in positie hebben, moeten hun processen herzien. De algemene verordening gegevensbescherming vereist specifiek dat organisaties geschikte technische en organisatorische maatregelen nemen om het verlies van of toegang door onbevoegden tot persoonlijke gegevens te voorkomen.

De algemene verordening gegevensbescherming (GDPR) is de meest omvattende en wereldwijd belangrijkste verordening ter beveiliging van persoonlijke gegevens.[1]

Dit roept bij velen vragen op, zoals:

V. Wat zijn persoonlijke gegevens?
A. Informatie in verband met een geïdentificeerde of identificeerbare natuurlijke persoon.[6] Dit kan identificators omvatten (zoals een naam of een identificatienummer) of gegevens over ras of etnische afkomst, politieke meningen, religie of filosofie, lidmaatschap van vakbonden, genetische gegevens, gezondheidsgegevens, criminele overtredingen; voorspellingen van werkprestaties, economische situatie, persoonlijke voorkeuren of interesses, betrouwbaarheid van gedrag, locatie of verplaatsingen enz.[7]

V. Wat is pseudonimiseren en wat heeft dat met mij te maken?
A. In de algemene verordening gegevensbescherming wordt 15 keer 'pseudonimiseren' gebruikt – een procedure waarbij identificatievelden in een gegevensrecord worden vervangen door één of meer kunstmatige identificators of pseudoniemen. In de algemene verordening gegevensbescherming wordt de toepassing van pseudonimiseren van persoonlijke gegevens aanbevolen om het risico voor gegevenssubjects te reduceren zodat beheerders en verwerkers kunnen voldoen aan hun verplichtingen inzake gegevensbescherming.[8]

V. Kunnen organisaties individuen om toestemming vragen om hun persoonlijke gegevens te vergaren?
A. Ja, maar deze toestemming moet worden gegeven door een duidelijke, bevestigende handeling die een vrijwillige, specifieke, geïnformeerde en ondubbelzinnige indicatie geeft van de toestemming van het gegevenssubject voor de verwerking van persoonlijke gegevens. Reeds aangevinkte hokjes, stilte en inactiviteit gelden niet als toestemming.[9] Organisaties moeten de ontvangen toestemming bijhouden en ervoor zorgen dat het verzoek om toestemming steeds kan worden onderscheiden van andere verzoeken, met gebruik van duidelijke, eenvoudige taal.[10] In artikel 13 wordt uitgebreide informatie uiteengezet die aan het gegevenssubject moet worden gegeven ten tijde van het vergaren van de persoonlijke gegevens, zoals het doel van het vergaren van de gegevens, de ontvangers of categorieën ontvangers van de persoonlijke gegevens en de periode van de opslag van de gegevens.

V. Wat is Privacy Effect Beoordeling (DPIA; Data Protection Impact Assessment)?
A. Voor activiteiten met een hoog risico is een Privacy Effect Beoordeling vereist, zodat organisaties de oorsprong, aard, bepaaldheid en ernst van de risico's kunnen beoordelen en passende maatregelen kunnen nemen om de risico's te beperken, zoals door codering. Bij de beoordeling van het risico van gegevensbeveiliging moet rekening worden gehouden met de risico's die worden veroorzaakt door de verwerking van persoonlijke gegevens, zoals accidentele of onwettige vernietiging, verlies, wijziging, onbevoegde vrijgave van of toegang tot de persoonlijke gegevens die worden verzonden, opgeslagen of op andere wijze worden verwerkt en die kunnen leiden tot fysieke, materiële of immateriële schade.[11]

V. Moet ik een speciale functionaris voor gegevensbescherming (DPO) aanstellen?
A. De aanstelling van een functionaris voor gegevensbescherming is verplicht wanneer de gegevensverwerking wordt uitgevoerd door een openbare autoriteit (behalve rechtbanken die uit hoofde van hun justitiële capaciteit handelen) en voor bedrijven waarvan de kernactiviteiten bestaan uit de verwerkingsprocedures waarbij gegevenssubjects regelmatig en systematisch op grote schaal moeten worden gecontroleerd. Een functionaris voor gegevensverwerking is tevens verplicht voor alle ondernemingen die op grote schaal gevoelige gegevens verwerken, zoals over gezondheid, religie en politieke meningen. Specifiek geldt voor de functionaris voor gegevensbescherming dat:

- deze op basis van beroepskwaliteiten wordt aangesteld, en in het bijzonder van deskundige kennis van de wetten en praktijken inzake gegevensbescherming
- deze een personeelslid of een externe dienstverlener kan zijn
- de contactgegevens aan de relevante gegevensbeschermingsautoriteit moeten worden verschaft
- deze moet worden voorzien van de van toepassing zijnde middelen om zijn/haar taken uit te voeren en zijn/haar deskundigheid te handhaven
- deze direct verslag uit moet brengen aan het hoogste bestuur
- deze geen andere taken mag uitvoeren die tot een belangenconflict zouden kunnen leiden.[12]

Vereisten inzake fysieke beveiliging en privacy
Wat moeten organisaties doen om data-inbreuk te voorkomen?
In artikel 24 van de algemene verordening gegevensbescherming wordt de verantwoordelijkheid van de organisatie uiteengezet om 'geschikte technische en organisatorische maatregelen' in te voeren om een correcte verwerking van persoonlijke gegevens te verzekeren en te demonstreren. In artikel 32 wordt nog een stap verder gegaan met de verklaring dat 'bij de beoordeling van de passende mate van beveiliging rekening moet worden gehouden met de risico's van de verwerking, en met name van accidentele en onwettige vernietiging, verlies, verandering, onbevoegde vrijgave van of toegang tot de persoonlijke gegevens die worden verzonden, opgeslagen of op andere wijze worden verwerkt'.

Een belangrijk aspect van dit voorschrift is de nadruk op de preventie van toegang door onbevoegden. Dit is waar fysieke beveiliging essentieel is. Het kan gegevens specifiek beschermen tegen interne en externe bedreigingen door mensen die willen profiteren van de spleten in de wanden van uw organisatie en via uw personeel. Dit omvat de beperking van de gegevens die kunnen worden geobserveerd, gestolen en benaderd. Bekijk het volgende en beoordeel of uw personeel de nodige technische en organisatorische maatregelen in positie heeft om eraan te voldoen.

Voer gegevensbescherming in via ontwerp en als standaard:
Om gegevens standaard te beschermen, moeten organisaties op proactieve wijze uitsluitend persoonlijke gegevens identificeren en vergaren die nodig zijn voor de beoogde doeleinden, de gegevens uitsluitend zo lang als nodig is bewaren (minimisatie principe) en moeten zij er vervolgens voor zorgen dat de persoonlijke gegevens niet beschikbaar worden gesteld aan een onbepaald aantal mensen. Dit zal waarschijnlijk betekenen, dat de risico's voor de privacy vooraf worden geïdentificeerd en dat er systemen worden ontworpen om deze risico's te beperken, naar behoeven met pseudonimiseren en anonimiseren, binnen de verwerkingsfuncties en het identificeren van specifieke mensen of functies die toegang moeten hebben tot de gegevens. Vraag uzelf af: Overweegt u de privacy risico's voor individuen voorafgaand aan het ontwerpen van uw informatiesystemen, bedrijfspraktijken en het fysieke ontwerp? Heeft u ontmoetingen gehad met uw IT-personeel om de huidige systemen en verwerkingsactiviteiten te herzien, om te bespreken of er nog andere stappen nodig zijn om te documenteren hoe persoonlijke gegevens door de gehele levensduur van gegevens zullen worden beschermd?

Gebruik fysieke veiligheidsmaatregelen:
Cyber beveiligingsmaatregelen zoals gegevenscodering en complexe wachtwoorden zijn kritisch, maar 'laagtechnische' administratieve en fysieke controles zijn even belangrijk. Om vast te stellen waar fysieke barrières nodig zijn, moet u vaststellen waar gevoelige gegevens worden benaderd. Bijvoorbeeld bij medewerkers die regelmatig mobiele apparatuur gebruiken om gegevens op allerlei plaatsen te openen en door te geven. Steeds meer van deze arbeiders benaderen gevoelige informatie in het openbaar, vaak in het volle zicht van anderen. Ook op kantoor stijgt het risico van de blootstelling van gegevens. In de zo populaire open kantoren zijn geen fysieke barrières meer die vroeger hielpen om computerschermen af te schermen. Vraag uzelf af: Zijn de computerschermen zo geplaatst dat ze niet naar ramen, deuren en openbaar toegankelijke ruimten zijn gericht? Zijn de beeldschermen van computers en mobiele apparatuur van privacyschermen voorzien om te voorkomen dat anderen de gegevens kunnen zien? Staan gemeenschappelijke printers/kopieermachines/ faxmachines in beschermde gebieden of kunnen ze worden afgesloten? Worden fysieke kopieën van gegevens op een plaats bewaard met een gecontroleerde toegang? Worden er standaard shredders geplaatst bij alle machines, vooral bij kopieermachines, printers en faxmachines, en is het een vereiste voor allen die telewerk doen of verbindingen op afstand gebruiken om bedrijfsinformatie te benaderen?

Training van medewerkers plannen:
Trainingsprogramma's moeten drie belangrijke aspecten bevatten: Observatie, fysieke toegang en beste praktijken inzake de preventie van diefstal. Medewerkers moeten er bijvoorbeeld aan worden herinnerd om zich bewust te zijn van hun omgeving bij het in het openbaar openen en werken via hun laptop, tablet en smartphone met verbonden apparatuur. De beeldschermen mogen niet blootgesteld zijn aan voorbijgangers en mogelijke toeschouwers, vooral bij het invoeren van logingegevens en het bekijken van de gegevens van gevoelige details. Wat betreft fysieke toegang moeten organisaties hun medewerkers opleiden om gegevens van white boards te wissen en na een vergadering de vertrouwelijke documenten te vergaren, hun wachtwoorden uit het hoofd te leren in plaats van ze op te schrijven, archiefkasten en laptops te vergrendelen, privacy-filters te gebruiken op computerapparatuur en hun bureau leeg te houden, inclusief afmelding van onbeheerde apparatuur. Vraag uzelf af: Omvat uw trainingsprogramma bewustzijn van de omgeving zodat uw medewerkers leren om rekening te houden met hun omgeving en verdacht gedrag kunnen herkennen en daarop kunnen reageren? Begrijpen uw medewerkers wat er van hen wordt verwacht wat betreft het beleid van een 'leeg bureau'? Herinnert u uw medewerkers regelmatig aan de goede praktijken inzake beveiliging die zij moeten volgen?

Duidelijke beleidslijnen opstellen:
Om te demonstreren dat de organisatie is toegewijd aan de invoering van de nodige maatregelen inzake beveiliging en privacy. De beleidslijnen moeten uiteenzetten wat er wel en niet mag in verband met de inzage en het gebruik, zowel door medewerkers als contractanten, zowel in de werkplaats als bij het werken op afstand. De arbeidscontracten moeten specifieke terminologie bevatten over de verantwoordelijkheid om gevoelige en vertrouwelijke gegevens veilig te houden.[13] Vraag uzelf af: Heeft u iedereen op de hoogte gesteld van uw privacy- en beveiligingsverklaring, met uitleg hoe uw organisatie persoonlijke gegevens beschermt, deelt, wegdoet en de toegang daartoe geeft? Wat is uw beleid inzake BYOD (bring your own device) dat het gedrag van werknemers en de vereiste beveiligingsmaatregelen bepaalt wanneer zij bedrijfsinformatie via hun eigen apparatuur benaderen? Vereist u als onderdeel van uw beveiligingsbeleid dat medewerkers zowel visuele controles als die op het gebied van cybersecurity gebruiken?

Limieten stellen voor gegevensopslag:
Bepaal maximale tijdperiodes voor de opslag van persoonlijke gegevens – in overeenstemming met de van toepassing zijnde wetten. Verwijder grondig alle persoonlijke gegevens die niet absoluut vereist zijn voor de doeleinden van het bedrijf waarvoor zij werden vergaard. Vraag uzelf af: Welke technische controles heeft u om ervoor te zorgen dat gegevens op de juiste tijd worden gewist? Voldoen de vernietigingsprocessen van uw organisatie aan de strenge beveiligingsrichtlijnen, zoals verschaft door NIST Special Publication 800-88, zoals het fysiek vernietigen van harde schijven die niet meer worden gebruikt?

Externe leveranciers verifiëren:
Gebruik uitsluitend verwerkers die voldoende garantie geven wat betreft expertise, betrouwbaarheid en middelen om technische en organisatorische maatregelen in te voeren, inclusief voor de beveiliging van de verwerking. Vraag uzelf af: Heeft u een verkopersbeheerprogramma in positie inclusief contractuele verplichtingen, met een overzicht voor het management van activiteiten van derden met toegang tot persoonlijke gegevens?

Stel een protocol op voor data-inbreuk:
Organisaties moeten bereid zijn om zonder onnodige vertraging de toezichthoudende autoriteit op de hoogte te stellen van een eventuele inbreuk in verband met persoonlijke gegevens (indien mogelijk binnen 72 uur). Of ze moeten kunnen aantonen dat het niet waarschijnlijk is dat de inbreuk in verband met persoonlijke gegevens een risico zal vormen voor de rechten en vrijheden van natuurlijke personen. Bij een hoog risico moeten tevens de gegevens instanties op de hoogte worden gesteld van de data-inbreuk, zonder onnodige vertraging.[14] Vraag uzelf af: Wanneer heeft u het laatst de beleidslijnen en planning van uw organisatie op het gebied van de respons op incidenten en de melding van een inbreuk herzien? Weten uw medewerkers wie zij binnen de organisatie op de hoogte moeten stellen bij een inbreuk op hun apparatuur of als zij zich bewust worden van data-inbreuk? Heeft u een bijgewerkt plan in positie inzake de respons op incidenten en de melding van inbreuk om te bepalen wanneer en hoe de autoriteiten op de hoogte moeten worden gesteld?

Ken de rechten van het individu:
Inwonenden van de EU hebben nu het recht om te zien welke persoonlijke gegevens organisaties over hen hebben – en in bepaalde omstandigheden om te vragen om hun gegevens te wissen. Dit recht van wissen vereist organisaties om alle links met, en kopieën en reproducties van die persoonlijke gegevens te wissen. Organisaties moeten een manier ter beschikking stellen waarop mensen elektronisch verzoeken in kunnen dienen, vooral als de persoonlijke gegevens op een elektronische manier worden verwerkt.[15] Vraag uzelf af: Weet uw organisatie wat er bedoeld wordt met 'persoonlijke gegevens' en hoe ze moeten reageren op vragen in verband met persoonlijke gegevens?

Conclusie:

De algemene verordening gegevensbescherming (GDPR) is de belangrijkste wijziging in de voorschriften inzake gegevensprivacy in 20 jaar. Deze schrijft voor dat persoonlijke gegevens op een zodanige manier worden beheerd, dat die de nodige veiligheid en vertrouwelijkheid bevordert – een taak die zowel technische als organisatorische beveiligingsmaatregelen vereist. En de boetes voor overtredingen kunnen verwoestend zijn. De voorbeelden die in de verordening uiteen worden gezet, zijn gewoon goede gang van zaken. Niemand wil dat hun gegevens worden misbruikt en geen organisatie wil de problemen van een data-inbreuk. Organisaties die de naleving van de privacy niet als een last zien, maar als zakelijke verantwoordelijkheid, kunnen er strategisch hun voordeel mee doen om hun reputatie en merkwaarde te verbeteren, betere medewerkers aan te trekken en uiteindelijk het vertrouwen van het publiek te handhaven.

www.3M.nl/privacyfilters of www.3M.be/privacyfilters

[1] Forrester, Lessons Learned from the World's Biggest Security Breaches and Data Abuses, 9 januari 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, the GDPR, 2017
[5] Ponemon Institute, The Impact of Data Breaches on Reputation & Shared Value, gesponsord door Centrify, 2017.
[6] Artikel 4, the GDPR, 2017
[7] Citaat 75, the GDPR, 2017
[8] Citaat 26 en 28, the GDPR, 2017
[9] Citaat 32, the GDPR, 2017
[10] Artikel 7, the GDPR, 2017
[11] Artikel 35 en Recital 83-84, the GDPR, 2017
[12] Artikel 37-38, the GDPR, 2017
[13] Citaat 74, 77-78, the GDPR, 2017
[14] Citaat 81, the GDPR, 2017
[15] Citaat 59, 63, 65, 66, the GDPR, 2017

The experts in screen privacy. | 3M