Privacy en security: treft u passende maatregelen?

Whitepaper voor (IT-)managers en privacyprofessionals

kpn. Het netwerk van Nederland

Dit zijn privacy en security

Het Nationaal Cyber Security Centrum (NCSC) omschrijft (cyber)security als ‘alle beveiligingsmaatregelen die men neemt om schade te voorkomen door een storing, uitval of misbruik van een informatiesysteem of computer.’ Ook bij privacy draait het om organisatorische en technische maatregelen. Hier moeten de maatregelen ervoor zorgen dat bijvoorbeeld klanten ‘onbespied en onbewaakt’ door het leven kunnen. Deze ‘bescherming van de persoonlijke levenssfeer’ is zelfs in de grondwet vastgelegd.

Inhoud

Inleiding

In het huidige digitale tijdperk doen we steeds meer zaken online. We videobellen met familie, vrienden en collega's, plannen online een afspraak in bij het ziekenhuis of de garage en regelen de weekboodschappen vanuit de luie stoel.

Risico's nemen toe

Het internet – met de daarbij behorende mogelijkheden – is niet meer weg te denken. Deze ontwikkeling brengt echter ook risico's met zich mee. Veel van onze (persoons)gegevens zijn inmiddels online te vinden en daarmee worden de risico's op misbruik van deze gegevens groter. De Autoriteit Persoonsgegevens luidde in maart 2021 zelfs de noodklok: de privacywaakhond zag in 2020 een explosieve toename van het aantal hacks gericht op het buitmaken van persoonsgegevens.[1]

De datalekken die daar het gevolg van zijn, halen regelmatig het nieuws. Zo kwam LinkedIn negatief in de publiciteit toen bleek dat de gegevens van 700 miljoen gebruikers werden aangeboden op een hackerforum.[2] Dichter bij huis was bijvoorbeeld de Nederlandse fastfoodketen New York Pizza slachtoffer van datadiefstal. De gegevens van 3,9 miljoen klanten werden buitgemaakt, waaronder e-mailadressen, telefoonnummers en bezorgadressen.[3] Cybercriminelen kunnen deze gegevens op vele manieren misbruiken, bijvoorbeeld voor ransomware-aanvallen.

Passende maatregelen

Digitale criminaliteit zit in de lift en zal de komende jaren blijven toenemen. Het waarborgen van de beschikbaarheid, integriteit en vertrouwelijkheid van data binnen organisaties staat onder druk. Daarmee wordt privacy een steeds belangrijker onderwerp, met name voor het management. Organisaties zijn bij wet verplicht om zorgvuldig om te gaan met persoonsgegevens. Doen ze dat onvoldoende, dan riskeren ze een boete van de AP.

De AP kan deze boete opleggen onder de Algemene verordening gegevensbescherming (AVG) die sinds mei 2018 van kracht is, en waaraan verwerkingsverantwoordelijken en verwerkers moeten voldoen. Volgens de AVG dienen ze 'passende maatregelen' te nemen om de persoonsgegevens die ze verwerken te beschermen. Maar hoe zien die maatregelen eruit? Wat is de relatie met security? En wanneer heeft u afdoende maatregelen getroffen? Die vragen beantwoorden we in deze whitepaper.

De relatie tussen privacy en security

'Security' en 'privacy' zijn termen die vaak in één adem worden genoemd. Toch zijn er wel degelijk verschillen. Bij 'security' gaat het meestal over informatiebeveiliging: het beveiligen van alle data en informatieprocessen binnen een organisatie. Privacy draait om de bescherming van de persoonlijke levenssfeer waar alle burgers recht op hebben. Hier ligt de focus op persoonsgegevens, of persoonlijk identificeerbare informatie (PII).

Er is nog een verschil. Vanuit security kunnen we vaak zelf bepalen welke risico's we accepteren, en welke niet. En dus ook welke maatregelen we nemen, en hoeveel geld we daaraan willen besteden. Uiteraard wordt de keuze hier en daar wel beperkt door wetgeving. Bij privacy is er echter veel minder keuzevrijheid. Wetgeving verplicht tot het treffen van maatregelen en klanten verwachten dat organisaties al het mogelijke doen om de privacy te beschermen.

Maar naast verschillen is er ook een duidelijke relatie tussen privacy en security. Privacy en security kijken beide naar de risico's die een verwerking van (persoons) gegevens met zich meebrengt. Op basis van deze risico's wordt bepaald of, en zo ja welke 'passende maatregelen' er genomen moeten worden. Dat zijn zowel organisatorische als technische (security)maatregelen. Daarmee komen privacy en security heel dicht bij elkaar te liggen.

[1] https://www.autoriteitpersoonsgegevens.nl/nl/nieuws/ap-luidt-noodklok-explosieve-toename-hacks-en-datadiefstal
[2] https://www.privacysharks.com/exclusive-700-million-linkedin-records-for-sale-on-hacker-forum-june-22nd-2021/
[3] https://nos.nl/artikel/2383364-fors-datalek-bij-new-york-pizza-3-9-miljoen-klantgegevens-gestolen

Wat zegt de AVG over passende maatregelen?

Artikel 25 van de AVG verplicht verwerkingsverantwoordelijken en verwerkers om voor de bescherming van persoonsgegevens passende maatregelen te nemen. We hebben het dan over 'privacy by design' en 'privacy by default'.[4]

De European Data Protection Board (EDPB), het Europees Comité voor gegevensbescherming, heeft artikel 25 verder uitgelegd in haar richtsnoeren 'Data Protection by Design and Default' (DPbDD). Deze richtsnoeren geven ook richting aan hoe artikel 25 toe te passen. We noemen een aantal kernpunten:

- Het beschermen van persoonsgegevens is geen eenmalige actie, maar een continu proces dat regelmatig moet worden beoordeeld. Daarnaast dient vanaf het begin voldoende aandacht besteed te worden aan het nemen van voldoende beveiligingsmaatregelen.
- Beveiliging is van toepassing op zowel nieuwe als bestaande verwerkingen.
- Een verwerkingsverantwoordelijke – die bepaalt voor welk doel en hoe persoonsgegevens worden verwerkt – mag rekening houden met de kosten die het implementeren van maatregelen met zich meebrengt. Alternatieven die voldoende veiligheid bieden, mogen worden gebruikt.
- Het beschermen van gegevens moet op de agenda staan van verwerkingsverantwoordelijken en verwerkers, maar ook van leveranciers van producten die met persoonsgegevens te maken hebben. Leveranciers moeten hun deskundigheid gebruiken om hun klanten, met name het mkb, te helpen de beveiliging te waarborgen.

Het beschermen van persoonsgegevens is geen eenmalige actie maar een continu proces dat regelmatig moet worden beoordeeld'

[4] Zie voor meer informatie hierover: edpb_guidelines_201904_dataprotection_by_design_and_by_default

Wat zijn voorbeelden van passende maatregelen?

De AVG spreekt veelal over het nemen van ‘passende technische en organisatorische maatregelen’. Wat die maatregelen exact zijn, wordt er niet bij verteld. Wel worden in artikel 32 van de AVG een aantal voorbeelden gegeven:

a. **Pseudonimisering en versleuteling.** Dit zijn veelgebruikte maatregelen. Denk maar aan de data op een laptop of USB-stick die zijn versleuteld middels encryptie. Bij pseudonimisering worden de gegevens zo verwerkt dat de betrokkene zonder aanvullende gegevens niet is te identificeren. Deze aanvullende gegevens moet u apart bewaren en eveneens passend beschermen met technische en organisatorische maatregelen.

b. Garanderen **vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht.** Met name bij beschikbaarheid en veerkracht speelt het Business Continuity Management (BCM)-proces een grote rol. Organisatie moeten na een calamiteit zoals een ransomwarebesmetting de persoonsgegevens kunnen herstellen. Dit vraagt om een schone en consistente back-up die binnen een bepaalde tijd is terug te zetten.

c. **Het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen.** Hier wordt het kunnen herstellen na een calamiteit verplicht gesteld voor persoonsgegevens, ongeacht het incident. De AP noemt bijvoorbeeld tijdelijke onbeschikbaarheid van medische gegevens in een ziekenhuis een groot risico. Dit betekent dat een ziekenhuis voldoende maatregelen moeten nemen om gegevens binnen een acceptabele tijd – bijvoorbeeld binnen enkele uren – te kunnen herstellen.

d. **Een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking.** In de praktijk blijkt regelmatig dat er geen tijd of kennis aanwezig is voor het testen en controleren van procedures. Of dat men er helemaal niet bij stilstaat dat dit moet gebeuren. De AVG vereist een proces voor het op regelmatige basis toetsen van de maatregelen. Hiervoor kunt u een Information Security Management System (ISMS) gebruiken. Het is ook het overwegen waard om de beoordeling door een externe partij uit te laten voeren. Een externe partij kijkt vaak met andere ogen naar uw processen en heeft ervaring met het uitvoeren van audits.

Naast de bovenstaande maatregelen geeft lid 4 van artikel 32.1 AVG nog aan dat bijvoorbeeld medewerkers alleen gegevens mogen verwerken als ze daarvoor een instructie hebben gehad van de verwerkingsverantwoordelijke. Hier kan een arbeidscontract aan ten grondslag liggen. Wettelijke verplichtingen kunnen voor uitzonderingen zorgen.

Welke passende maatregelen moet ik treffen?

De AVG stelt dat de verwerkingsverantwoordelijke en verwerker passende maatregelen moeten nemen. Dit wil niet zeggen dat de verwerking 100 procent veilig moet zijn. Komt het na een overtreding tot een boete? Dan zal de AP bij het bepalen van de boete rekening houden met de technische en organisatorische maatregelen die de verwerkingsverantwoordelijke of de verwerker heeft getroffen.[5]

Risico-assessment

Belangrijk bij de beoordeling welke maatregelen u moet nemen, is dat u rekening houdt met de risico's voor de betrokkenen en de aard of gevoeligheid van de persoonsgegevens die u verwerkt. Uit lid 1 van artikel 32 van de AVG volgt dan ook dat u een risico-assessment moet doen. Hierbij dient u zelf de risico's te beoordelen die betrekking hebben op de verwerking. Een Data Protection Impact Assessment (DPIA, of 'gegevensbeschermingseffectbeoordeling') helpt u de risico's in te schatten. In sommige gevallen is het verplicht een DPIA uit te voeren.

Bij de risicoanalyse moet de verwerkingsverantwoordelijk of verwerker minimaal de volgende aspecten meenemen:[6]

- Stand van de techniek
- Aard van de verwerking
- Omvang en context van de verwerking
- Kosten van de maatregelen
- Doeleinden
- Impact van de risico's en de waarschijnlijkheid dat deze risico's voorvallen

[5] Zie art. 83.2 onderdeel d AVG
[6] Overweging 83 AVG

Hoe toon ik een ‘passende beveiliging’ aan?

Op het gebied van informatiebeveiliging zijn er verschillende normen waaronder de ISO 27001, NEN 7510-7513 en de BIO (Baseline Informatiebeveiliging Overheid). Als een organisatie voldoet aan een van deze normen, zijn de maatregelen dan ook goed genoeg om te voldoen aan artikel 32 van de AVG?

Normen als richtlijnen

Het is belangrijk om op te merken dat de Uitvoeringswet AVG niet vereist dat de verwerkingsverantwoordelijke of verwerker voldoet aan een van deze normen. Wel kunnen we uit jurisprudentie concluderen dat deze normen worden beschouwd als richtlijn als het gaat om het nemen van passende maatregelen.

Zo legde de AP een ziekenhuis een boete op voor het niet gebruiken van tweefactorauthenticatie en het niet regelmatig beoordelen van de logbestanden met betrekking tot de toegang tot de data[7]. Dit zijn eisen die gesteld worden in de NEN 7510- en 7513-normen. Ook geeft de AP op haar website aan dat een NEN 7510-certificaat niet verplicht is onder de AVG, maar dat u daarmee wel kunt tonen dat u de juiste organisatorische en technische maatregelen heeft genomen om aan de AVG te voldoen[8].

‘Beveiligingsnormen kunnen worden beschouwd als richtlijnen als het gaat om het nemen van passende maatregelen’

Gedragscodes en certificeringen

Een andere optie is het volgen van een goedgekeurde gedragscode (artikel 40 AVG) of een certificeringsmechanisme (art. 42 AVG) om aan te tonen dat de organisatie voldoet aan de eisen rondom de technische en organisatorische maatregelen.

Op het moment van schrijven zijn er echter nog geen certificeringen goedgekeurd en is er nog maar één gedragscode in Nederland. Dit is de ‘Data Pro Code’ die geschikt is voor kleinere verwerkers. Deze gedragscode is in 2020 onder voorbehoud goedgekeurd. Daarnaast is er een NEN ISO 27701 als toevoeging op de 27001. Dit is op dit moment echter nog geen norm waarmee compliance met de AVG kan worden aangetoond.

[7] De rechtbank Den Haag heeft de boete aangepast naar € 350.000, zie: ECLI:NL:RBDHA:2021:3090
[8] https://www.autoriteitpersoonsgegevens.nl/nl/onderwerpen/gezondheid/zorgverleners-en-de-avg

Wat kan KPN Security voor mij betekenen?

Als het gaat om de bescherming van persoonsgegevens komen privacy en security steeds dichter bij elkaar te liggen. Al bij het ontwerp van een proces voor de verwerking van persoonsgegevens moet u rekening houden met de privacy- en securityaspecten. Bepaal op basis van een risicoanalyse de juiste passende technische en organisatorische maatregelen en controleer met regelmaat of deze maatregelen nog steeds voldoen.

Het is daarbij belangrijk dat security- en IT-professionals regelmatig het gesprek aangaan met de privacy-officer, functionaris gegevensbescherming of een andere privacymedewerker binnen de organisatie. Zij kunnen adviseren over de privacyaspecten die bij de verwerking van toepassing zijn, en over de (effectiviteit van de) maatregelen. Maar ook KPN Security kan u hierin ondersteunen.

Vertrouwelijkheid is ons fundament

Het bewaken van de vertrouwelijkheid van communicatie is al meer dan een eeuw het fundament van onze onderneming. Wij beschermen naast uw ICT-infrastructuur ook uw (privacygevoelige) data, intellectueel eigendom, persoonlijke gegevens én uw reputatie. Onze klanten kunnen er altijd op rekenen dat privacy en veiligheid onze hoogste prioriteit hebben.

Met de ‘Maturity Scan’ maakt KPN Security inzichtelijk waar u staat als het gaat om privacy en security. Op basis daarvan kunt u een privacy- en een securitybeleid en een plan van aanpak opstellen. Als securityspecialist biedt KPN Security bovendien de technische maatregelen die nodig zijn om de privacy van uw klanten te beschermen. We staan u tijdens het gehele traject bij met advies en helpen bij de implementatie van zowel de organisatorische als technische beschermende maatregelen.

Kunnen we u ergens bij helpen?

Of heeft u interesse in de Maturity Scan?
Neem dan contact op via
➜ www.kpn.com/zakelijk/security/privacy

‘Met de ‘Maturity Scan’ maakt KPN Security inzichtelijk waar u staat als het gaat om privacy en security’

Over onze whitepapers

Onze experts publiceren regelmatig whitepapers waarin u onze visie terugvindt op actuele onderwerpen. Soms gaan ze over ICT-thema's, soms over thema's die daaraan raken. Deze whitepapers maken we om onze ervaring en expertise met u te delen. Om u te inspireren en te laten zien wat er anno nu allemaal mogelijk is. En raakt u aan de hand daarvan geïnteresseerd in ons en onze diensten?
Meer informatie daarover vindt u op ➜ kpn.com/security

AD-20457/10-21/KRE