De digitale videodeurbel, do or don't?

'**Detecteer bewegingen** wanneer iemand je terrein betreedt. **Ontvang meldingen** op je telefoon, tablet of pc. **Zie, hoor en spreek** bezoekers in realtime, waar je ook bent.'[1] Aldus Ring, een van de populairste merken in de beveiligingswereld. Dit klinkt voor veel consumenten als muziek in de oren. Want wie wil er nu niet weten wat er rondom zijn huis gebeurt en wie het terrein betreedt? Daarbij is het ook gewoon handig om de postbezorger op afstand te kunnen vertellen dat het pakketje in de tuin gezet mag worden. Maar zijn consumenten zich wel bewust van de juridische aspecten die de gadget met zich meebrengt? We lezen wel vaker dat er een goede reden moet zijn om een videocamera op te hangen of dat dit alleen mag wanneer het noodzakelijk is, maar wat wordt hier dan mee bedoeld en wat is uw rol als consument? Daar komt bij dat u als gebruiker ook privacyrisico's voor uzelf creëert. We zijn nieuwsberichten zoals: *'De app van de slimme deurbel Ring zit vol met trackers die persoonsgegevens versturen naar adverteerders'* [2] *en 'Vier Ring-medewerkers ontslagen om misbruiken gebruikersvideo's'* [3]*,* toch nog niet vergeten? De populaire gadget heeft dus twee kanten. Na het lezen van dit artikel kunt u als consument een weloverwogen keuze maken om de gadget wel, niet of op een verantwoorde manier te gebruiken.

Valt u onder de privacywet door een videodeurbel?
Door de digitale videodeurbel te installeren en te gebruiken, loopt u het risico om te moeten voldoen aan de Algemene Verordening Gegevensbescherming (AVG), de zogenoemde privacywet. U zult misschien denken dat u daar niet onder valt, u heeft de deurbel toch gewoon voor privégebruik? Echter, wanneer uw digitale videodeurbel een gedeelte van de openbare ruimte filmt, moet u wel degelijk voldoen aan alle verplichtingen uit de AVG. Om dit te voorkomen, moet u het bereik van de videodeurbel zo instellen dat alleen uw eigen terrein wordt gefilmd. Wanneer u in een woonwijk woont, wordt dit lastig. De deurbel filmt dan al snel een stuk van de stoep of straat mee en in dat geval valt de digitale videodeurbel wél onder de AVG. Daarbij komt ook dat u de gegevens niet mag delen op het internet. Hoewel de Ringapp een standaard functie heeft om de beelden via Whatsapp of Facebook te delen, wordt sterk aangeraden dit niet te doen. Wanneer u dit wel doet, valt de verwerking niet onder privégebruik en ook dan moet u aan de volgende verplichtingen voldoen.[4]

Waar moet u aan voldoen als u wel de openbare ruimte filmt?
Voordat u de digitale videodeurbel in gebruik neemt, dient u het doel van de verwerking schriftelijk vast te leggen. Dit doel kan het beschermen van uw eigendommen en terrein zijn. De verwerking van persoonsgegevens voor dit doel, moet te baseren zijn op een wettelijke grondslag. In de wet zijn verschillende grondslagen opgenomen, maar voor videocamera's wordt veelal toestemming van de betrokkene of de behartiging van een gerechtvaardigd belang gebruikt. Het aantonen van toestemming is gezien de aard van de videodeurbel, waarbij ook onbekende personen gefilmd worden, moeilijk te bewijzen. Daarom wordt aangeraden uw verwerking te baseren op de grondslag gerechtvaardigd belang.[5] Maar wat houdt dit dan precies in en wat moet u doen?

Ten eerste moet u een gerechtvaardigd belang hebben. Er is bepaald dat de bescherming van eigendommen een gerechtvaardigd belang is, maar dit belang moet wel actueel zijn.[6] Dit betekent dat er een situatie van nood moet zijn voordat u de digitale videodeurbel ophangt. Hierbij valt te denken aan een eerdere inbraak of het wonen in een wijk waar veel woninginbraken plaatsvinden.

---

[1] *Doorbells*, nl-nl.ring.com.
[2] *Slimme Ring deurbel stuurt stiekem data naar adverteerders*, 28 januari 2020, rtlnieuws.nl.
[3] *Vier Ring-medewerkers ontslagen om misbruiken gebruikersvideo's*, 9 januari 2020, nu.nl.
[4] The European Data Protection Board, *Guidelines 3/2019 on processing of personal data through video devices*, 29 januari 2020, edpb.europa.eu, p. 7-8.
[5] The European Data Protection Board, *Guidelines 3/2019 on processing of personal data through video devices*, 29 januari 2020, edpb.europa.eu, p. 14.
[6] The European Data Protection Board, *Guidelines 3/2019 on processing of personal data through video devices*, 29 januari 2020, edpb.europa.eu, p. 9-10.

Daarnaast moet u zich altijd afvragen of de videodeurbel geschikt is om uw doel te bereiken en of er geen minder ingrijpende maatregel is? U kunt bijvoorbeeld ook beveiligingssloten gebruiken om inbraak te voorkomen. Deze maatregel maakt in tegenstelling tot de videodeurbel geen inbreuk op de privacy van bezoekers. U dient deze overweging van tevoren te maken. De noodzaak eindigt in principe aan uw eigendomsgrens, maar aangezien een deel van de openbare ruimte filmen in veel gevallen onvermijdelijk is, dient u technische maatregelen te nemen om dit te beperken.[7] Zoals eerder besproken, kunt u de bewegingsdetector van de deurbel aanpassen. Zo kunt u precies bepalen wat noodzakelijk is voor uw doeleinde en de niet noodzakelijke gedeelten uitschakelen. U dient ook na te gaan welk soort gebruik noodzakelijk is. De deurbel van Ring is zowel met als zonder abonnement te gebruiken. Zonder abonnement heeft u een deurbel die alleen livebeelden vastlegt, maar met abonnement worden de beelden ook bewaard en opgeslagen.[8] Wanneer u alleen het voorkomen van inbraak als doeleinde hebt beschreven, is bepaald dat realtime-monitoring voldoende is.[9] Wanneer het abonnement wel noodzakelijk is voor uw doeleinde, moet u rekening houden met opslagbeperking. Het is belangrijk dat u de inhoud niet langer bewaart dan noodzakelijk is voor uw doeleinde. Als uw doel het beschermen van eigendommen is, kan schade vaak in 72 uur worden vastgesteld. Dit betekent dat langer bewaren in strijd zou zijn met de AVG. Als u de inhoud langer bewaart, moet u kunnen aantonen dat dit noodzakelijk was.[10]

Tot slot dient u de belangen van de personen die u filmt altijd af te wegen. Dit doet u door te kijken naar de gevolgen voor de betrokkenen en de ernst van de inbreuk die u op hun privacy maakt. Vervolgens dient u deze gevolgen te voorkomen of te beperken door bovenstaande punten in acht te nemen.[11]

Welke verplichtingen heeft u nog meer?
Als u aan alle bovenstaande voorwaarden heeft voldaan, dient u nog aan de volgende verplichtingen te voldoen.

Informatieplicht
U bent verplicht om personen te laten weten dat zij gefilmd worden door de digitale videodeurbel. Maar hoe moet u dit dan doen? U dient gebruik te maken van een waarschuwingsbord. Dit bord dient zo geplaatst te worden dat de personen op de hoogte zijn van de videodeurbel, voordat zij uw terrein betreden. U kunt het bord dus het beste bevestigen aan het begin van het bewaakte terrein, bijvoorbeeld op een poort. Het waarschuwingsbord moet de belangrijkste informatie bevatten, waaronder uw identiteit, het doel van de verwerking, de rechten van betrokkenen, maar ook of u de opnamen bewaart of deelt. Het waarschuwingsbord moet verwijzen naar bijvoorbeeld een link of een telefoonnummer, waar de personen meer informatie kunnen vinden.[12] De waarschuwingssticker die Ring meelevert, voldoet hier niet aan. U dient een ander bord te gebruiken of de sticker aan te vullen met deze informatie.

Beveiligingsplicht
Daarnaast bent u verplicht maatregelen te nemen om de verzamelde gegevens te beveiligen.[13] Dit dient u van tevoren al te doen. Hier komt de bewegingsdetector weer bij kijken. U dient deze zo privacyvriendelijk mogelijk in te stellen. Dit betekent dat u de detector instelt op de minimale afstand van 2 meter en dat u de gebieden waarop de openbare ruimte te zien is, uitzet in het bewegingsveld van de deurbel. Vervolgens moet u er alles aan doen om de verzamelde gegevens zo goed mogelijk te beveiligen. Dit doet u door in ieder geval:

[7] The European Data Protection Board, *Guidelines 3/2019 on processing of personal data through video devices*, 29 januari 2020, edpb.europa.eu, p. 11.
[8] *Protect plans*, nl-nl.ring.com.
[9] The European Data Protection Board, *Guidelines 3/2019 on processing of personal data through video devices*, 29 januari 2020, edpb.europa.eu, p. 11.
[10] The European Data Protection Board, *Guidelines 3/2019 on processing of personal data through video devices*, 29 januari 2020, edpb.europa.eu, p. 28.
[11] The European Data Protection Board, *Guidelines 3/2019 on processing of personal data through video devices*, 29 januari 2020, edpb.europa.eu, p. 11.
[12] The European Data Protection Board, *Guidelines 3/2019 on processing of personal data through video devices*, 29 januari 2020, edpb.europa.eu, p. 26-27.
[13] Artikel 25 en artikel 32 AVG.

- De tweestapsverificatie in de Ringapp uit te voeren;
- Een sterk en uniek wachtwoord te kiezen en deze af en toe te veranderen;
- Uw inloggegevens niet te delen met andere personen;
- Uw gekoppelde apparaat (bijvoorbeeld smartphone) te updaten en te beveiligen door een wachtwoord toe te voegen.[14]

Registerplicht

Tot slot bent u verplicht een verwerkingsregister bij te houden. U moet een overzicht van de verwerking kunnen overhandigen wanneer de Autoriteit Persoonsgegevens hierom vraagt. Dit overzicht moet de belangrijkste informatie bevatten, waaronder bijvoorbeeld uw contactgegevens en het doel van de verwerking.[15] Om het u gemakkelijk te maken, is een voorbeeld verwerkingsregister opgesteld.[16]

Wat gebeurt er als u deze verplichtingen niet nakomt?

Het verantwoord gebruiken van de digitale deurbel is niet voor niets. De Autoriteit Persoonsgegevens kan maatregelen opleggen. Hierbij kunt u denken aan een verwerkingsverbod waardoor u de videodeurbel niet meer mag gebruiken, maar ook een geldboete. Ook de personen die u filmt kunnen in actie komen. Zij kunnen een klacht indienen bij de toezichthoudende autoriteit, waardoor u wellicht moet stoppen met de verwerking en het gebruik van de videodeurbel. De betrokkene kan zich ook tot de rechter wenden en een schadevergoeding eisen voor de inbreuk op zijn rechten.[17] Dit is uiteraard allemaal niet wat u wilt en verwacht wanneer u een digitale videodeurbel aanschaft. Want zo'n digitale gadget is toch gewoon erg handig en leuk? Wanneer u de stappen uit dit artikel volgt en verantwoord met uw digitale videodeurbel omgaat, blijft de gadget dit ook. Deze stappen gelden nogmaals niet wanneer u de deurbel alleen voor privédoeleinden gebruikt en de openbare ruimte niet filmt. In dat geval loopt u wel de volgende andere privacyrisico's.

Overige risico's die u loopt, ook zonder de openbare ruimte te filmen

Tot slot brengt het gebruiken van de digitale videodeurbel van Ring ook risico's voor uw gegevens met zich mee. Uit de servicevoorwaarden en de privacyverklaring blijkt dat Ring meer doet met uw gegevens dan u misschien denkt. Ring kan onder andere uw gebruikersopnamen openen en gebruiken, uw gegevens doorverkopen of delen en uw gegevens overdragen naar andere landen.[18]

Verder is uit onderzoek gebleken dat Ring op bepaalde punten niet of niet geheel in overeenstemming handelt met de AVG. Zo weet u niet welke gegevens er voor welke doeleinden verwerkt worden. Het lijkt alsof uw gegevens op een stapel komen te liggen en Ring alle gegevens voor elk doeleinde kan gebruiken. Heel transparant kunnen we dit dus niet noemen. Uiteraard heeft ook Ring een wettelijke grondslag nodig om uw gegevens te mogen verwerken. Mede door gebrek aan informatie is er voor een aantal doeleinden geen wettelijke grondslag gevonden. Ook is het niet te achterhalen hoelang de gegevens worden opgeslagen. Er worden onduidelijke of zelfs geen opslagtermijnen gegeven. Tot slot valt er genoeg te zeggen over de beveiliging van Ring. Zoals in het begin van dit artikel al beschreven is, zijn er situaties gebleken waarin Ring onvoldoende bescherming heeft geboden. Inmiddels zijn er nieuwe veiligheidsmaatregelen geïntroduceerd, maar ook daar wordt veel verantwoordelijkheid bij u neergelegd. Zo dient u gepersonaliseerde advertenties, waarbij het merk uw gegevens deelt, zelf uit te schakelen in de Ringapp. Verder wordt sterk aangeraden uw gegevens te beschermen door de maatregelen te nemen zoals omschreven bij de beveiligingsplicht. Als u dit doet, kunt u de bescherming van uw gegevens voor een groot deel waarborgen en op een verantwoorde manier gebruik maken van de gadget.

---

[14] *Extra lagen beveiliging en controle,* 24 februari 2020, nl-nl.ring.com.
[15] B. W. Schermer, D. Hagenauw, N. Falot, *Handleiding Algemene verordening gegevensbescherming en Uitvoeringswet Algemene verordening gegevensbescherming,* 22 januari 2018, autoriteitpersoonsgegevens.nl, p. 52.
[16] Voorbeeld register.
[17] B. W. Schermer, D. Hagenauw, N. Falot, *Handleiding Algemene verordening gegevensbescherming en Uitvoeringswet Algemene verordening gegevensbescherming,* 22 januari 2018, autoriteitpersoonsgegevens.nl, p. 90-92.
[18] Servicevoorwaarden en privacyverklaring.