AUTORITEIT
PERSOONSGEGEVENS

Internet of things en smart home? Bescherm uw privacy!

Het aantal apparaten met een internetverbinding in Nederlandse huishoudens groeit met de dag. Bijvoorbeeld smart tv's, wearables (zoals een smartwatch), speelgoed, muzieksystemen, lampen en thermostaten. Deze internet of things-apparaten kunnen ons leven makkelijker maken, maar verzamelen ook veel privacygevoelige informatie. Dat kan een risico zijn.

Wilt u een internet of things-apparaat gaan gebruiken? Zorg er dan voor dat u uw privacy beschermt. Om u hierbij te helpen, geeft de Autoriteit Persoonsgegevens (AP) in deze handleiding een aantal tips voor het kopen, installeren en gebruiken van een internet of things apparaat.

Kopen

Lees de privacyverklaring

Internet of things-apparaten verzamelen gegevens die veel over u en anderen kunnen zeggen. Het is belangrijk dat u van tevoren weet wat er met deze gegevens gebeurt als u een apparaat gaat gebruiken. Zodat u zelf kunt beslissen of u dat wel wilt.

Kijk op de website van de fabrikant van het apparaat voor de privacyverklaring. Die moet makkelijk te vinden zijn. En makkelijk te lezen en begrijpen. De fabrikant moet u onder meer de volgende informatie geven:

- hoe u bij vragen contact kunt opnemen met het bedrijf;
- welke persoonsgegevens het bedrijf van u verwerkt;
- waarom het bedrijf dat doet (voor welk specifiek doel);
- of het bedrijf uw gegevens buiten de Europese Unie (EU) verwerkt;
- of het bedrijf uw gegevens deelt met of doorverkoopt aan andere partijen en zo ja, aan welke.

Ook moet het bedrijf u wijzen op uw privacyrechten en hoe u die kunt gebruiken. Meer weten? Zie dossier Recht op informatie.

Kijk naar de beveiliging

Ga op zoek naar de beveiliging van het apparaat. Dit doet u door te zoeken naar:

- Betrouwbare tests.
- Eventuele bekende veiligheidsrisico's.
- Ervaringen van andere gebruikers.
- De garanties die de fabrikant geeft voor bijvoorbeeld toekomstige software -updates. Geeft de fabrikant geen duidelijke informatie over de veiligheid van het product? Of kunt u de informatie niet vinden? Vraag er dan naar bij de fabrikant of de (web)winkel.

Kijk naar de (web)winkel en fabrikant

Kijk goed naar welk product u bij welke (web)winkel koopt. Let daarbij niet alleen op de prijs. Soms zijn producten van buiten de EU een goedkoop alternatief. U kunt zo'n product makkelijk zelf online kopen bij een (web)winkel buiten de EU of tijdens een vakantie kopen en mee nemen naar huis.

Maar dit kan wel privacyrisico's met zich meebrengen. Soms is het bijvoorbeeld lastig of onmogelijk uw privacyrechten uit te oefenen bij (web)winkels die buiten de EU zijn gevestigd.

Koopt u een apparaat zonder EU-goedkeuringen? Dan haalt u een product in huis dat niet gegarandeerd aan de Europese standaarden moet voldoen. Daardoor kunnen de beveiliging en de garantie van het product tekortschieten.

Ook kunnen apparaten uw gegevens doorsturen naar servers buiten de EU, terwijl dat niet zomaar mag. Dit privacyrisico is nog groter als kwetsbare personen het apparaat gebruiken, zoals kinderen of mensen met een beperking.

Of als het apparaat gevoelige gegevens van u registreert, zoals gegevens over uw gezondheid of over uw financiën. Daarnaast kan uw apparaat ook gegevens van en over anderen dan uzelf registreren, zoals uw huisgenoten, buurtgenoten, bezoekers of passanten.

Geeft de fabrikant van het apparaat dat u wilt kopen geen duidelijke informatie? Bijvoorbeeld over de beveiliging (zoals software-updates) of hoe u het apparaat privacyvriendelijk kunt instellen? Vraag dit dan na bij de (web)winkel waar u het product wilt gaan kopen. Bent u niet tevreden met het antwoord? Vraag dan welk ander apparaat u kunt kopen dat wél veilig en privacyvriendelijk is.

Installeren

Verander uw wachtwoord en gebruikersnaam

Het veranderen van uw wachtwoord en, als dat kan, uw gebruikersnaam is een van de belangrijkste stappen in het beveiligen van (nieuwe) apparatuur. Blijf nooit een door de fabrikant ingesteld wachtwoord gebruiken.

Kies voor een lang wachtwoord dat of een 'wachtzin' die verschillende soorten tekens combineert. U kunt ook een wachtwoordmanager gebruiken om uw wachtwoorden te beheren en nieuwe sterke wachtwoorden te genereren.

Gebruik meerfactorauthenticatie

Vaak logt u in met een gebruikersnaam en een wachtwoord. Maar biedt het apparaat of platform meerfactorauthenticatie? Dan is het aan te raden dat te gebruiken, zeker als het apparaat gevoelige gegevens registreert. Hierdoor is het apparaat of uw account beter beveiligd tegen ongeautoriseerde toegang.

Meerfactorauthenticatie houdt in dat u naast uw gebruikersnaam en wachtwoord nog iets anders nodig heeft om toegang te krijgen. Bijvoorbeeld een code die u krijgt per sms of app. Of soms een hardwaresleutel.

Stel uw (online) account in

Veel fabrikanten maken gebruik van een (online) account of app waarin u instellingen kunt wijzigen. Neem de tijd om deze instellingen te doorlopen. En de privacygevoelige instellingen goed in te stellen.

Stel het apparaat af

Apparaten kunnen ook gegevens van en over anderen dan uzelf opvangen. Bijvoorbeeld geavanceerde microfoons gekoppeld aan spraakherkenningssystemen. Stel het apparaat zo af dat het de privacy van anderen niet aantast. Houd bij camera's rekening met de privacyregels voor cameratoezicht.

Gebruiken

Beveilig uw router

Uw router is de toegangspoort van uw apparaten naar het internet. De standaardinstellingen van uw router maken u mogelijk kwetsbaar voor digitale indringers of voor het lekken van uw gegevens.

Zorg daarom voor een sterk wachtwoord. Pas daarnaast de instellingen van uw router aan, zodat die passen bij uw persoonlijke situatie. Bijvoorbeeld: maakt u geen gebruik van de functionaliteit om van buiten uw huis toegang te krijgen tot uw router of netwerk? Schakel die functionaliteit dan uit.

Blijf software en apps updaten

De veiligheid van internet of things-apparaten is ook afhankelijk van de software op het apparaat en van de software die het apparaat aanstuurt. Zorg dat u altijd de meest recente software (of app) heeft geïnstalleerd, zodat eventuele bekende kwetsbaarheden gerepareerd worden.

Zijn er geen automatische updates beschikbaar? Kijk dan op de website van de fabrikant of u de meest recente versie heeft. Controleer na een update de instellingen van het apparaat. Zo bent u er zeker van dat privacyvriendelijke instellingen niet zijn overschreven door de update.

Is de software sterk verouderd en zijn er geen updates meer? Dan kan het apparaat een beveiligingsrisico gaan vormen. Overweeg om het apparaat te vervangen.

Vervangt u het apparaat? Of gebruikt u het niet meer? Verwijder dan uw gegevens die op het apparaat staan. Dit doet u door het apparaat te resetten naar de fabrieksinstellingen. Of door handmatig uw gegevens te wissen. Verwijder ook eventueel aanwezige geheugenkaarten of opslagschijven.

Wat te doen bij problemen

Beveiligingsprobleem

Internet of things-apparaten worden op grote schaal geproduceerd en verkocht. Dat betekent dat een beveiligingsprobleem bij een veel gekocht apparaat of type apparaat een grote groep mensen kan raken.

Hoort u in de media dat er een beveiligingsprobleem is dat mogelijk uw apparatuur betreft? Dan kunt u voor meer informatie het beste de website van de fabrikant raadplegen.

U kunt ook het apparaat tijdelijk uitschakelen tot duidelijk is wat het probleem is en hoe u het apparaat weer veilig kunt gebruiken.

Vraag of klacht

Heeft u een vraag of een klacht over uw privacy bij een internet of things-apparaat? Ga dan in eerste instantie naar de fabrikant van het apparaat.

Heeft u een klacht en komt u er samen met de fabrikant of (web)winkel niet uit? Dan kunt u een privacyklacht indienen bij de Autoriteit Persoonsgegevens (AP). Als het apparaat gemaakt is in de EU of u het in de EU gekocht heeft, kan de AP eventueel verdere stappen ondernemen.