

Privacyvisie

Inleiding

Iedereen heeft wel iets waarvoor hij/zij zich schaamt. De een peutert in de neus, de ander heeft een bepaalde seksuele fetisj en weer een ander is in het geheim een hele grote fan van Nicki Minaj. Deze dingen wil je niet graag aan mensen vertellen, maar er zijn ook andere redenen dan schaamte alleen om dingen niet te zeggen. Zo kun je bijvoorbeeld bang zijn dat je gepest of uitgelachen wordt of omdat je gewoon gelooft dat het andere mensen niet aangaat.

Aan de andere kant zijn er misschien andere dingen die je wel graag wilt vertellen aan andere mensen, zoals bijvoorbeeld het feit dat je bent gaan hardlopen deze week, of dat je cum laude bent geslaagd van je middelbare school, of dat je een nieuwe lamborghini hebt gekocht, of noem maar op.

Het belangrijkste is dat jij een recht hebt om aan andere mensen over jezelf te vertellen wat jij wilt. En dat recht hebben wij gelukkig. Het is namelijk het recht op privacy. Dit recht staat verankert in de grondwet, het Europees verdrag voor de rechten van de mens en de Universele verklaring voor de rechten van de mens.

De SP-Hilversum staat daarom pal voor het recht op privacy van de burgers van Hilversum en vindt het daarom ook van belang dat de gemeente Hilversum transparant is met betrekking tot hoe zij gegevens van de inwoners verwerkt. In dit stuk gaat de SP-Hilversum haar visie op het privacy beleid van de gemeente uiteenzetten.

Dataminimalisatie

De gemeente heeft als taak om niet meer gegevens van personen te verzamelen dan noodzakelijk voor de uitvoer van haar taken. Dit concept heet dataminimalisatie. De gemeente moet transparant zijn welke gegevens zij verzamelt en om welke reden. De vragen die gesteld moeten worden zijn: wat is de toegevoegde waarde van deze verzamelde persoonsgegevens? weegt die waarde op tegen de gevolgen van de schending van het privacyrecht? En wat voor voordeel hebben de inwoners hierbij? In concreto betekent dit: is het volgen van mensen door wifi wel noodzakelijk? Moet daar wel een camera komen? En moeten we wel vragen of iemand man of vrouw is?

Toestemming en andere reden om gegevens te verwerken

Verwerken van gegevens betekent niet anders dan alles wat je met gegevens kunt doen, bijvoorbeeld verzamelen, vernietigen en delen met anderen. Om gegevens van mensen te verwerken moet daar een duidelijke reden voor zijn. Soms is er in de wet een reden om gegevens te verwerken. Soms moeten er gegevens verwerkt worden omdat een contract moet worden uitgevoerd. En soms moet er toestemming worden gevraagd. In de mening van de SP-Hilversum hoeft de gemeente alleen toestemming te vragen van inwoners als er geen andere reden is om gegevens te verwerken. Hierdoor is er minder papierwerk nodig dan in het geval dat er altijd om toestemming wordt gevraagd.

Transparant

De gemeente dient transparant te zijn met welke gegevens zij verwerkt. Dit is wettelijk verplicht. Een gemeentelijke privacy verordening die democratisch is vastgesteld zorgt hiervoor.

Informatieverstrekking

Burgers dienen goed te geïnformeerd worden over welke gegevens er worden verzameld en wat er met die gegevens wordt gedaan. Dit is wettelijk verplicht, maar gebeurt nauwelijks. Volgens een rapport van de autoriteit persoonsgegevens (AP) over de toestemming in het sociaal domein: “Verder lijken veel gemeenten de burger uitsluitend te informeren over de verwerking van persoonsgegevens in situaties waarin daarvoor toestemming wordt gevraagd. Er lijkt niet te zijn voorzien in een procedure om te voldoen aan de informatieplicht in situaties waarin er geen toestemming wordt gevraagd voor de verwerking van persoonsgegevens.”¹

Maar ook de mensen die in de dienst zijn van de gemeente moeten goed geïnformeerd zijn over de privacywetgeving zodat zij de burgers kunnen informeren over hun rechten. De AP constateert dat deze kennis onvoldoende aanwezig is bij professionals die werkzaam zijn in het sociaal domein: “Deze professionals zijn echter niet voorzien van werkinstructies waarin de wettelijke vereisten voor het informeren van betrokkenen bij de verwerking van hun persoonsgegevens in het sociaal domein, op consistente en heldere wijze zijn vertaald naar de praktijk.”¹

Veiligheid en datalekken

Als de gemeente gegevens verzameld, moeten die gegevens ook op een zorgvuldige wijze worden opgeslagen. Er moet onderzoek, zogenoemde DPIA, worden gedaan naar de gevolgen voor de privacy en de veiligheidsrisico's van nieuwe processen waarbij gegevens van burgers worden verzameld. Ieder vermoede van een inbreuk waarbij gegevens zijn bemachtigd moet gelijk onderzocht worden. Als zo een inbreuk heeft plaatsgevonden moet daar gelijk op gehandeld worden zodat de gevolgen voor de burgers klein is. Verder moet in dat geval de AP ook geïnformeerd worden.

Sociaal domein

Ook in het sociaal domein worden veel gegevens van burgers verwerkt. In dat geval gaat het ook vaak om privacygevoelige gegevens, zoals een medisch dossier of financiële gegevens, en zijn de mensen ook kwetsbaar en afhankelijk van de gemeente. Daarom moet de gemeente alles eraan doen om de privacy van deze kwetsbare burgers te waarborgen. Het moet deze burgers duidelijk zijn wie hun gegevens inziet en wat hun rechten zijn met betrekking tot hun privacy.

Camera's

Overall in ons dorp zijn camera's. Een aantal zijn door de gemeente in het centrum geplaatst met als doel de openbare orde te handhaven en de veiligheid te bevorderen. Het plaatsen van deze camera's is geregeld in de APV.

Er zijn ook camera's opgehangen door private partijen, bijvoorbeeld in bedrijfsterrein. Deze camera's kunnen in de openbare ruimte zijn opgehangen, of filmen (delen) daarvan. De SP-Hilversum begrijpt waarom private partijen camera's plaatsen, maar dit ontslaat de gemeente niet van haar taak om voor de privacy van de burgers te zorgen. Er moeten duidelijke afspraken komen van hoe er met de camerabeelden worden omgegaan. Voor camera's die er nu al hangen is er een overgangsperiode van 3 jaar, dan moeten de afspraken zijn gemaakt.

Open data

Open data is data waarop geen auteursrecht rust en bekostigd is met openbare middelen. Deze data dient openbaar te zijn. Deze data mag geen gegevens bevatten die herleidbaar zijn naar een persoon.

Gemeentelijke organisatie

In de gemeentelijke organisatie dient ook aandacht te bestaan voor privacy. Daarom moet in ieder organisatieonderdeel een contactpersoon zijn die belast is met de coördinatie en uitvoering van het privacy- en beveiligingsbeleid van het betreffende organisatieonderdeel. Verder moet er volgens de wet ook een functionaris voor de gegevensbescherming worden benoemd. Deze dient op onafhankelijke wijze onderzoek te kunnen doen naar en toezicht te kunnen houden op de gemeente.

De gemeente zal verder ook geen gebruik maken van Blockchain technologie om persoonsgegevens te verwerken. Blockchain is heel transparant, omdat alle transacties openbaar zijn. Als voorbeeld kijken we naar de Bitcoin, een cryptomunt die gebruik maakt van Blockchain. Iedereen weet wat de rest met deze munt heeft gekocht. Dit schreeuwt niet echt privacy. Aangezien de gemeente heel veel privacygevoelige gegevens heeft, is het niet wenselijk om dit door middel van Blockchain op te slaan.

Bronnen

1: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/toestemmingsrapport_definitief_incl_bijlagen.pdf