Deelvraag 5

Researchdocument

13-11-2023

Inhoud

Aanleiding 3
Methode 4
Resultaat 5
Conclusie 9
Bronnen 10

Aanleiding

Uit het interview met de jeugdwerkers van Dynamo is gebleken dat zij tijdens hun werk zich niet altijd aan de huidige AVG-wetgeving kunnen houden. De informatie die zij binnenkrijgen over de jongeren waarmee zij werken, verkrijgen zij niet altijd op de correcte manier.

Veel informatie die zij binnenkrijgen over jongeren hebben ze te horen gekregen via andere jongeren, terwijl deze informatie officieel alleen maar met toestemming van de ouders/ verzorgers mag komen. Hierdoor kunnen ze deze informatie niet in een officieel dossier zetten.

Toch geven ze aan dat deze informatie mondeling gedeeld wordt met elkaar, ze zitten dan wel met de vraag “moeten we dit wel doen” maar geven ook aan dat ze er zitten met het doel om jongeren te helpen.

Verder waren ze ook in aanraking gekomen met de AVG-wetgeving toen ze het idee hadden om posters met QR-codes op te hangen in hun buurt, om een groepswhatsapp te maken voor de jongeren. Echter ging dit niet door omdat iedereen dan de mogelijkheid had om hieraan mee te doen zonder dat ze goed konden controleren wie er allemaal in de groep zou zitten. Hierdoor was er een risico dat minderjarige samen in een groep met volwassenen kwamen te zitten.

Daarom gaven de Jeugdwerkers van Dynamo aan dat het soms lastig is om jeugdwerk te doen volgens de regels van de AVG-wetgeving. Maar omdat ze zichzelf daar wel zoveel mogelijk aan willen houden zijn we tijdens het gesprek samen tot conclusie gekomen dat het nuttig is om richtlijnen te creëren voor jongerenwerkers waarbij het makkelijker wordt om er rekening mee te houden.

Methode

We hebben een Expertinterview gehad met Dynamo om te vragen over de problematiek van jongeren en wat eraan gedaan kan worden. Wij vroegen Dynamo over de privacy van jongeren en hoe Dynamo hier mee omgaat. Ook wilden we graag weten hoe de AVG wet invloed heeft op het werk van Dynamo.

We hebben ook online onderzoek gedaan met behulp van Literature Study. We zijn de wetgeving door gaan lezen om te onderzoeken hoe de privacywetgeving precies in elkaar zit en waar jeugdwerkers op moeten letten als het gaat om de jeugd.

Resultaat

Om jeugdwerkers bewust te maken van de privacywetgeving hebben we een aantal belangrijke punten uitgelijnd. Met deze punten hebben de jeugdwerkers de belangrijkste richtlijnen waar ze rekening mee kunnen houden tijdens hun werk. Het is belangrijk dat jeugdwerkers veilig omgaan met gegevens van jongeren en dat zij de toestemming hebben.

1. **Toestemming**:

Zorg ervoor dat je toestemming hebt van ouders of wettelijke voogden voordat je persoonlijke gegevens van kinderen onder de 16 jaar verzamelt, verwerkt of deelt. De leeftijd kan per provincie variëren maar is nooit lager dan 13. Vanaf 16 jaar kan de desbetreffende persoon zelf toestemming geven.

Er moet ook extra rekening mee gehouden worden dat het niet is toegestaan (zonder uitdrukkelijke toestemming van de persoon zelf of voogd) om persoonlijke informatie te verwerken waaruit iemands ras, etnische afkomst, politieke opvattingen, religie, levensbeschouwelijke overtuigingen, genetische gegevens, biometrische gegevens voor unieke identificatie, gezondheidsinformatie, of informatie over iemands seksueel gedrag of seksuele voorkeur blijkt.

2. Doelbeperking, transparantie en dataretentie:

Definieer duidelijk het beoogde doel van gegevensverzameling. Bijvoorbeeld, als je contactgegevens verzamelt voor evenementregistratie, gebruik deze dan niet voor andere doeleinden zonder opnieuw toestemming te vragen.

a) Persoonsgegevens moeten op een manier worden verwerkt die voor de betrokken persoon rechtmatig, behoorlijk en transparant is (dit wordt "rechtmatigheid, behoorlijkheid en transparantie" genoemd).

b) De gegevens moeten worden verzameld voor specifieke, duidelijk omschreven en gerechtvaardigde doeleinden. Ze mogen niet verder verwerkt worden op een manier die niet overeenkomt met die oorspronkelijke doeleinden. Uitzonderingen zijn onder andere archivering in het algemeen belang, wetenschappelijk of historisch onderzoek, of statistische doeleinden (dit noemen we "doelbinding").

c) De verzamelde gegevens moeten voldoende, relevant en beperkt zijn tot wat noodzakelijk is voor de doeleinden waarvoor ze worden verwerkt (dit is "minimale gegevensverwerking").

d) De gegevens moeten juist zijn en zo nodig worden bijgewerkt. Als gegevens onjuist zijn, moeten alle redelijke maatregelen worden genomen om ze onmiddellijk te corrigeren of te verwijderen (dit heet "juistheid").

e) De gegevens moeten worden bewaard in een vorm die het mogelijk maakt om de betrokken personen niet langer te identificeren dan nodig is voor de oorspronkelijke doeleinden. Het is echter toegestaan om gegevens voor langere tijd op te slaan voor archivering in het algemeen belang, mits passende technische en organisatorische maatregelen worden genomen om de privacy te beschermen (dit staat bekend als "opslagbeperking").

f) De verwerking van gegevens moet op een veilige manier plaatsvinden. Er moeten passende technische of organisatorische maatregelen worden genomen om de gegevens te beveiligen tegen ongeautoriseerde toegang, verlies, vernietiging of beschadiging (dit wordt "integriteit en vertrouwelijkheid" genoemd).

De organisatie die verantwoordelijk is voor de gegevensverwerking moet ervoor zorgen dat deze principes worden nageleefd en moet dit kunnen aantonen (dit wordt "verantwoordingsplicht" genoemd).

3. Rechten van betrokkenen:

Benadruk dat oudere kinderen mogelijk zelf hun rechten kunnen uitoefenen, zoals het recht op toegang tot hun gegevens of het recht om vergeten te worden.

Als een bedrijf/ organisatie direct digitale diensten aanbiedt aan een kind en er toestemming is, is het legaal om persoonlijke gegevens van het kind te verwerken als het kind minstens 16 jaar oud is. Als het kind jonger is dan 16 jaar, is deze verwerking alleen legaal als de persoon die verantwoordelijk is voor het kind toestemming heeft gegeven. (Zie punt 1: Toestemming)

De organisatie die verantwoordelijk is voor de gegevensverwerking moet redelijke inspanningen leveren om, rekening houdend met beschikbare technologie, te controleren of de persoon die verantwoordelijk is voor het kind toestemming heeft gegeven.

4. Beveiliging:

Onderstreep het belang van sterke wachtwoorden, versleuteling van gegevens en het regelmatig bijwerken van beveiligingsmaatregelen om persoonsgegevens te beschermen.

De organisatie die verantwoordelijk is voor de verwerking van persoonsgegevens en de partij die deze gegevens verwerkt, moeten passende maatregelen nemen om ervoor te zorgen dat de beveiliging in lijn is met het risico. Dit omvat onder andere:

a) Het gebruiken van technieken zoals versleuteling van persoonsgegevens.

b) Het zorgen voor permanente bescherming van de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten.

c) Het vermogen om snel de beschikbaarheid van en toegang tot persoonsgegevens te herstellen in geval van een fysiek of technisch incident.

d) Het regelmatig testen, beoordelen en evalueren van de effectiviteit van technische en organisatorische maatregelen die zijn genomen om de verwerking te beveiligen.

Bij het bepalen van het juiste beveiligingsniveau wordt specifiek gekeken naar de risico's van de verwerking, met name in gevallen van vernietiging, verlies, wijziging, ongeoorloofde verstrekking of toegang tot de verwerkte gegevens, zowel per ongeluk als onrechtmatig.

Het aansluiten bij een goedgekeurde gedragscode of een goedgekeurd certificeringsmechanisme kan dienen als bewijs dat aan de beveiligingseisen wordt voldaan.

Personen die onder het gezag van de organisatie handelen en toegang hebben tot persoonsgegevens, moeten deze alleen verwerken op instructie van de organisatie, tenzij er een wettelijke verplichting is om dit te doen.

5. Meldplicht datalekken:

Als er iets fout gaat met persoonlijke gegevens, moet degene die verantwoordelijk is voor de gegevensverwerking dit zo snel mogelijk melden aan de toezichthoudende autoriteit. Dit moet binnen 72 uur gebeuren, tenzij het niet waarschijnlijk is dat de fout een groot probleem is voor de mensen waarvan de gegevens zijn.

Als het niet lukt om binnen 72 uur te melden, moet er een reden voor de vertraging worden gegeven.

Als er een fout met persoonlijke gegevens is, moet degene die de gegevens verwerkt, zo snel mogelijk de persoon die verantwoordelijk is voor de gegevensverwerking informeren zodra hij op de hoogte is van de fout.

Bij de melding van de fout moeten in ieder geval de volgende dingen worden verteld:

a) Wat voor fout er is gemaakt met de persoonlijke gegevens, inclusief welke groepen mensen en welke soorten gegevens het betreft, en ongeveer hoeveel mensen en gegevens het zijn.

b) De naam en contactgegevens van de persoon die verantwoordelijk is voor gegevensbescherming of een ander contactpunt waar meer informatie kan worden verkregen.

c) Wat waarschijnlijk de gevolgen zijn van de fout met persoonlijke gegevens.

d) Welke maatregelen de persoon die verantwoordelijk is voor de gegevens heeft voorgesteld of genomen om de fout met persoonlijke gegevens op te lossen, inclusief eventuele maatregelen om de schade te beperken.

Als het niet mogelijk is om alle informatie tegelijk te geven, mag de informatie in stappen worden gegeven, maar dit mag geen onnodige vertraging veroorzaken.

Degene die verantwoordelijk is voor de gegevensverwerking moet alle fouten met persoonlijke gegevens documenteren, inclusief wat er is gebeurd, wat de gevolgen waren en welke corrigerende maatregelen zijn genomen. Dit helpt de toezichthoudende autoriteit te controleren of de regels zijn nageleefd.

6. Impactbeoordeling gegevensbescherming (**DPIA**):

Geef concrete voorbeelden van activiteiten die een hoog risico kunnen vormen voor de privacy van minderjarigen, zoals het gebruik van nieuwe technologieën of het profileren van gegevens.

Als er een bepaald soort gegevensverwerking plaatsvindt, vooral wanneer nieuwe technologieën worden gebruikt, en het lijkt erop dat dit een groot risico met zich meebrengt voor de rechten en vrijheden van mensen, dan moet degene die verantwoordelijk is voor de gegevensverwerking vooraf een beoordeling maken van hoe dit de bescherming van persoonlijke gegevens kan beïnvloeden. Dit geldt ook als er een reeks vergelijkbare verwerkingen zijn met vergelijkbare hoge risico's.

Als er een functionaris voor gegevensbescherming is aangesteld, moet degene die verantwoordelijk is voor de gegevensverwerking advies vragen aan deze functionaris wanneer zo'n beoordeling wordt uitgevoerd.

Een beoordeling is met name nodig in de volgende situaties:

a) Er wordt op een systematische en uitgebreide manier gekeken naar persoonlijke aspecten van mensen, gebaseerd op geautomatiseerde verwerking, inclusief profilering, met besluiten die rechtsgevolgen hebben voor de betrokkenen of hen op vergelijkbare wijze aanzienlijk beïnvloeden.

b) Grootschalige verwerking van bijzondere categorieën persoonsgegevens, zoals gezondheidsgegevens, of gegevens met betrekking tot strafrechtelijke veroordelingen en strafbare feiten.

c) Er is sprake van systematische en grootschalige monitoring van openbaar toegankelijke ruimten.

De toezichthoudende autoriteit maakt openbaar voor welke soorten verwerkingen een beoordeling verplicht is en deelt deze lijst met het relevante Comité.

De toezichthoudende autoriteit kan ook een lijst opstellen en openbaar maken van verwerkingen waarvoor geen beoordeling vereist is.

7. Direct contact opnemen met jongeren

Tijdens het werk kunnen Jeugdwerkers het nodig vinden om direct contact op te nemen met jongeren waarvan ze zien dat er iets speelt op de online platformen waar ze op aanwezig zijn.

Omdat tijdens dit proces van onlinehulp aanbieden soms de vraag naar voren komt: Gaan de jongeren wel reageren op een bericht van een onbekend persoon, of vinden de jongeren het misschien raar dat ze hulp worden aangeboden van een ouder en onbekend persoon?

Adviseren we om het duidelijk te maken dat ze met een jeugdwerker te maken hebben, doe dit niet alleen door het te vermelden maar ook door een socialmedia account te gebruiken die alleen gebruikt wordt met de functie jeugdwerk en geen privé account.

Wettelijk gezien is dit niet verplicht maar dit kan voor meer zekerheid zorgen bij de jongeren dat ze contact hebben met iemand met de juiste intenties.

Conclusie

We zijn van plan om de relevante wetgeving en richtlijnen op onze website te plaatsen, zodat jeugdwerkers er gemakkelijk toegang toe hebben wanneer dat nodig is. We hebben onze prototypes aan Fenna gepresenteerd, en ze was heel positief over de voorgestelde toevoegingen. Fenna zij dat dit op dit moment geen prioriteit heeft. Desondanks blijven we werken aan de implementatie van deze informatie op de website, zodat het beschikbaar is voor raadpleging wanneer het team er klaar voor is.

Bronnen

https://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=CELEX:32016R0679&qid=1685451198313#d1e3874-1-1