jongerenwelzijn

nota

nota aan alle medewerkers van Jongerenwelzijn
naam lijnmanager Stefaan De Vos
naam auteur Linda Van Weyenberg
onderwerp **Algemene richtlijn inzake persoonsgegevens van minderjarigen in e-mailberichten**

Update: Algemene richtlijn inzake persoonsgegevens van minderjarigen in e-mailberichten

Brussel, 2 april 2015.

Deze aangepaste nota is bedoeld om duidelijkheid te verschaffen en om te komen tot een meer pragmatisch voorstel inzake het omgaan met de gegevens en namen van minderjarigen in e-mails. De vorige nota is besproken op de verschillende managementorganen van het agentschap, wat heeft geleid tot een aantal aanpassingen. Zo wordt nu een duidelijk onderscheid gemaakt tussen intern en extern e-mailverkeer.

Wat het **interne e-mailverkeer** betreft – naar personen met een e-mailadres dat eindigt op @jongerenwelzijn.be of @wvg.vlaanderen.be – is er géén nood aan extra beveiliging aangezien dit reeds voldoende is ingebouwd in onze systemen.

Voor **e-mails naar derden** (iedereen wiens e-mailadres NIET eindigt op @jongerenwelzijn.be of @wvg.vlaanderen.be) gelden wel aparte regels. Dat moet de verspreiding van e-mails tegengaan waarin (on)rechtstreeks identificeerbaar over jongeren wordt gecommuniceerd op een onbeveiligde manier.

Sommige e-mails bevatten namen of gedetailleerde situatieschetsen van jongeren zonder verdere beveiliging. Medewerkers vertrekken veelal vanuit de – foute - idee dat enkel (een combinatie van) naam, voornaam, geboortedatum of het rijksregisternummer persoonsgegevens zijn die beveiligd moeten worden. Hiervoor steunen ze op de Privacywet– die omschrijft hoe we op een juiste manier persoonsgegevens moeten verwerken.

Artikel 1 § 1.
*Voor de toepassing van deze wet wordt onder "**persoonsgegevens**" **iedere informatie betreffende een geïdentificeerde of identificeerbare natuurlijke persoon verstaan**, hierna "betrokkene" genoemd; als identificeerbaar wordt beschouwd een persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificatienummer of van één of meer specifieke elementen die kenmerkend zijn voor zijn of haar fysieke, fysiologische, psychische, economische, culturele of sociale identiteit.*

Dat betekent inderdaad dat (een combinatie van) naam, voornaam, geboortedatum of het rijksregisternummer persoonsgegevens zijn aangezien deze iemand identificeerbaar maken. Volgens de Privacywet zijn er evenwel **veel meer gegevens** persoonsgegevens. Ook andere metadata over een persoon kunnen namelijk tot identificatie leiden, bv. M.X. (initialen) uit voorziening XYZ is duidelijk herleidbaar tot één persoon, of bv. zelfs Bavo als erg unieke voornaam kan tot identificatie leiden. De Privacywet stelt zelfs dat als iemand direct of indirect kan worden geïdentificeerd, alle gegevens die daarbij staan dan ook persoonsgegevens zijn. Zo kan bv. het banale gegeven 'schoenmaat' een persoonsgegeven zijn als dit bij een identificeerbaar persoon staat.

Verder in de Privacywet hebben artikels 6, 7 en 8 het over **gevoelige persoonsgegevens**. Ook daarvoor gelden er strengere eisen voor de verwerking. Het gaat hier dan over:

*Artikel 6: § 1. De verwerking van persoonsgegevens waaruit de **raciale of etnische afkomst, de politieke opvattingen, de godsdienstige of levensbeschouwelijke overtuiging of het lidmaatschap van een vakvereniging blijken, alsook de verwerking van persoonsgegevens die het seksuele leven betreffen**, is verboden.*
(in § 2 wordt dan omschreven wanneer dit wel kan)

*Artikel 7: § 1. De verwerking van persoonsgegevens die de **gezondheid** betreffen, is verboden.*
(in § 2 wordt dan omschreven wanneer dit wel kan)

*Artikel 8: § 1. De verwerking van persoonsgegevens inzake **geschillen voorgelegd aan hoven en rechtbanken alsook aan administratieve gerechten, inzake verdenkingen, vervolgingen of veroordelingen met betrekking tot***

***misdrijven, of inzake administratieve sancties of veiligheidsmaatregelen**, is verboden.*
(in § 2 wordt dan omschreven wanneer dit wel kan)

Volgens art. 16 van de Privacywet moet de **verwerking van persoonsgegevens** daarenboven gebeuren volgens de gepaste technische en organisatorische maatregelen, voor de bescherming ervan tegen toevallige of ongeoorloofde vernietiging, tegen toevallig verlies, evenals tegen de wijziging van of de toegang tot, en iedere andere niet toegelaten verwerking van persoonsgegevens.

Samengevat

Persoonsgegevens van een minderjarige moeten steeds op een juiste manier beveiligd worden. Deze gegevens zonder extra beveiliging e-mailen buiten onze e-maildomeinen is niet zo'n beveiliging! E-mail buiten onze emaildomeinen biedt namelijk veel van de vereiste beveiligingsmaatregelen **niet**.

Hoe kunnen we via e-mail persoonsgegevens uitwisselen?

- **Binnen onze e-maildomeinen (@jongerenwelzijn.be en @wvg.vlaanderen.be**). Omdat e-mails tussen collega's onze e-mailomgeving niet verlaten en omdat eventuele foutieve adressen door onze eigen e-mailbeheerder worden opgevangen, is het toegelaten om naar collega's met een e-mailadres binnen onze e-maildomeinen persoonsgegevens te versturen, zonder bijkomende beveiliging.

  Let er evenwel op:

  - dat enkel de juiste en nodige bestemmelingen deze persoonsgegevens krijgen,
  - je niet onnodig veel details verstuurt,
  - iedereen in To-veld, CC-veld en BCC-veld tot onze e-maildomeinen behoort, anders geldt onderstaande regeling i.v.m. e-mails 'Buiten onze e-maildomeinen'.

- **Buiten onze e-maildomeinen (inclusief e-mail naar andere e-maildomeinen van de Vlaamse overheid, bv. @ond.vlaanderen.be**). Het uitwisselen van persoonsgegevens via e-mail naar bestemmelingen buiten onze e-maildomeinen is enkel mogelijk door encryptie van de bijlagen. In het onderwerp en de verdere e-mail mogen verder geen (in)direct identificeerbare persoonsgegevens worden vermeld.

  Encryptie is mogelijk met een compressie-programma en daar de optie 'encrypteer' te kiezen. Het gebruikte wachtwoord moet dan via een ander kanaal dan e-mail aan de bestemmeling van de e-mail worden bezorgd. Hoe het wachtwoord wordt bepaald en hoe dat wordt meegedeeld aan de correspondent, gebeurt volgens afspraken binnen de teams.

Mogelijke programma's voor encryptie zijn:

- Izarc
  http://www.izarc.org/: dit pakket is standaard in gebruik bij Jongerenwelzijn, handleiding zie intranet;
- WinZip
  http://kb.winzip.com/kb/entry/109;
- 7-zip
  http://socialwork.columbia.edu/sites/default/files/file_manager/pdfs/Using%207-Zip%20for%20Encryption%205-30-2013.pdf.

Wie dit wenst, kan een beroep doen op de IT-aanspreekpunten voor technische ondersteuning.

Bij deze vraag ik met aandrang om deze richtlijn met de grootste nauwgezetheid toe te passen.

Stefaan Van Mulders
Administrateur-generaal Jongerenwelzijn