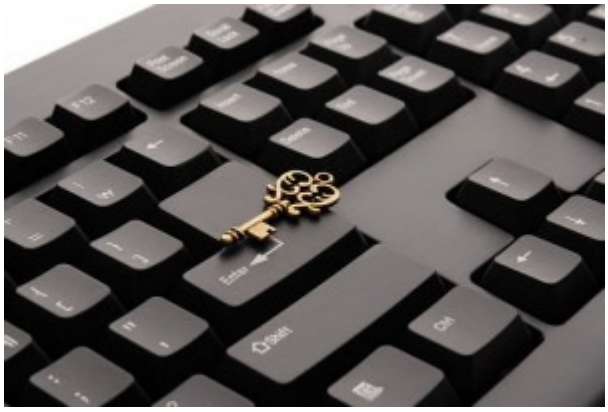
Meldplicht datalekken, is jouw organisatie er klaar voor?

Een briefje met dieetwensen van de kinderen op een keukendeurtje waar ook alle ouders langslopen, is dat een datalek? En als de ouders de gegevens van hun kind willen inzien, mag dat? De nieuwe Europese privacywetgeving AGV die mei volgend jaar ingaat roept genoeg vragen op om een middag mee te vullen.



Het is druk in het zaaltje in Purmerend waar vanmiddag de workshop 'Meldplicht datalekken' wordt gegeven. Het grootste deel van de middag is ingeruimd voor advocaten Calorien Brederije en Natascha Niewold van Valegis advocaten om de aanwezigen bij te praten over de nieuwe en aangescherpte regels van de Algemene verordening gegevensbescherming (AVG) die op 25 mei 2018 ingaat.
De AVG is de nieuwe Europese privacywetgeving en vervangt de huidige Wet bescherming persoonsgegevens (Wbp). Deze wetgeving brengt meer verplichtingen mee voor werkgevers en meer rechten voor werknemers en ouders van kinderen. De AVG is al sinds mei 2016 in werking, maar zal volgend jaar echt toegepast worden waarmee de Wbp verdwijnt.
De Meldplicht datalekken, die sinds 1 januari 2016 van kracht is en waarbij ernstige datalekken gemeld moeten worden bij de Autoriteit Persoonsgegevens (AP) zal onder deze nieuwe wetgeving strengere eisen krijgen.

Zwervende gegevens
De middag begint met een kort filmpje van een Belgisch televisieprogramma waarin mensen bij een waarzegger aanschuiven. Deze waarzegger weet verdacht veel over zijn 'gasten'; eerst noemt hij namen van goede vrienden en de kleur van een motor, maar al snel horen ze hoeveel geld ze deze maand aan kleding hebben uitgegeven en hoeveel ze rood staan. Doodeng. De waarzegger blijkt dan ook hulp van hackers achter een gordijn te krijgen. Moraal van het verhaal: we beseffen niet hoeveel persoonlijke informatie er online te vinden is over ons.
En daarmee is de toon gezet. Want met de digitalisering van bedrijven en organisaties en de hoeveelheid (persoonsgebonden) data die digitaal verwerkt worden, ontstaat ook het gevaar op misbruik of lekken van data, bedoeld en onbedoeld. Hacks, onnadenkende werknemers die wachtwoorden uitwisselen, gestolen of vergeten laptops, verkeerd verstuurde e-mails, noem maar op en er zit een risico aan.
Organisaties die zich bezighouden met het verwerken van persoonsgegevens krijgen er dus wat verantwoordelijkheden bij om de privacy van deze gevoelige gegevens te waarborgen. Dat geldt zeker ook voor organisaties in de kinderopvang die zowel met de

registratie van gegevens van werknemers als met de registratie van gegevens van kinderen een behoorlijke hoeveelheid persoonsgegevens verwerken.

Persoonsgegevens, wat moet je ermee?

Wat betreft de verwerking van persoonsgegevens blijft veel hetzelfde onder de AVG. Een aparte categorie zijn de bijzondere persoonsgegevens. Of een kind een dieetwens heeft bijvoorbeeld vanwege een godsdienst of medische aandoening. Hiervoor geldt een hoge mate van bescherming. Een organisatie mag geen bijzondere persoonsgegevens verwerken, tenzij dat noodzakelijk is met het oog op een zwaarwegend algemeen belang. Onder de AVG is het nog belangrijker om te inventariseren welke bijzondere persoonsgegevens worden verwerkt en of deze verwerking op een rechtsgeldige grondslag berust. En deze gang van zaken (hoe worden de gegevens verwerkt) te documenteren in voorschriften.

Dan heb je het bijvoorbeeld over briefjes met dieetwensen van de kinderen die op de kastdeurtjes hangen. Deze gegevens zijn namelijk direct herleidbaar naar een persoon en vertellen iets over iemands geloofsovertuiging of medische status.

Volgens Brederije en Niewold is zo'n lijstje niet direct een datalek, maar moet er wel een andere oplossing voor gezocht worden om deze informatie te verwerken. Eén waarbij de gezondheid van het kind niet in het geding is, maar ouders en andere onbevoegde personen deze informatie niet kunnen zien.

Een ander voorbeeld gaat over vaccinatiegegevens. Stel dat een bezorgde ouder vraagt of er kinderen niet gevaccineerd zijn in de klas, dan mag je antwoorden met ja of nee, maar zodra de informatie te herleiden is naar een specifiek kind mag je deze informatie niet geven onder de privacywetgeving.

Hetzelfde geldt voor het verwerken van gegevens van kinderen online. Bijvoorbeeld via een app, online game, webwinkel of via sociale media (denk aan foto's van een schooluitje). Bij kinderen onder de 16 jaar mag dit alleen als de ouders hiervoor (schriftelijk) toestemming hebben gegeven. En die toestemming moet per onderdeel gevraagd worden. Met alleen een 'ja' op het inschrijfformulier bij de vraag: Mogen we foto's op internet gebruiken', ben je volgens de AVG niet correct bezig. Per uitje, per foto, per medium moet er toestemming komen.

Documentatieplicht

Een belangrijke verandering in de AVG is de verantwoordingsplicht van persoonsgegevens. Nu is er nog een meldplicht, waarbij er voor de kinderopvang een vrijstelling voor de kinderen is, maar die vervalt met de komst van de AVG. Dat betekent dat een organisatie moet kunnen aantonen en onderbouwen dat de verwerking van de persoonsgegevens in overeenstemming is met de bepalingen van de AVG.

Kortom, iedereen moet een privacy-administratie bijhouden. Doe je dit niet, dan levert dat niet alleen een waarschuwing op maar ook een boete die kan oplopen tot miljoenen euro's.

Die registratie begint al wanneer een ouder een kind inschrijft. Papiertjes worden (soms handgeschreven of uitgeprint) ingevuld en ingeleverd bij een leider en die moet een

protocol hebben hoe dit wordt opgeborgen. Heb je dit niet, dan ben je niet goed bezig volgens de Autoriteit Persoonsgegevens (AP). Paspoort, BSN, rekeningnummer, alles staat op deze inschrijving. Het is daarom heel belangrijk dat dit veilig wordt verwerkt. En dat geldt niet alleen voor inschrijvingen, maar bijvoorbeeld ook of iedere werknemer wel een eigen wachtwoord heeft voor de bedrijfs-iPad tot aan de toestemming van ouders voor het gebruik van foto's online (zoals hierboven beschreven moet je voor alles een gedocumenteerde toestemming hebben). Iedere handeling moet kunnen worden verantwoord.
Wanneer je hier op voorhand een geschreven protocol voor hebt, ben je in ieder geval voorbereid, is het devies en de aanbeveling van de dames Brederije en Niewold. Neem hierin op wie met welk informatiesysteem welke persoonsgegevens verwerkt. Welke beveiligingsmaatregelen er zijn genomen om de gegevens te beschermen. En of kan worden aangetoond dat deze maatregelen doeltreffend en effectief zijn geweest.

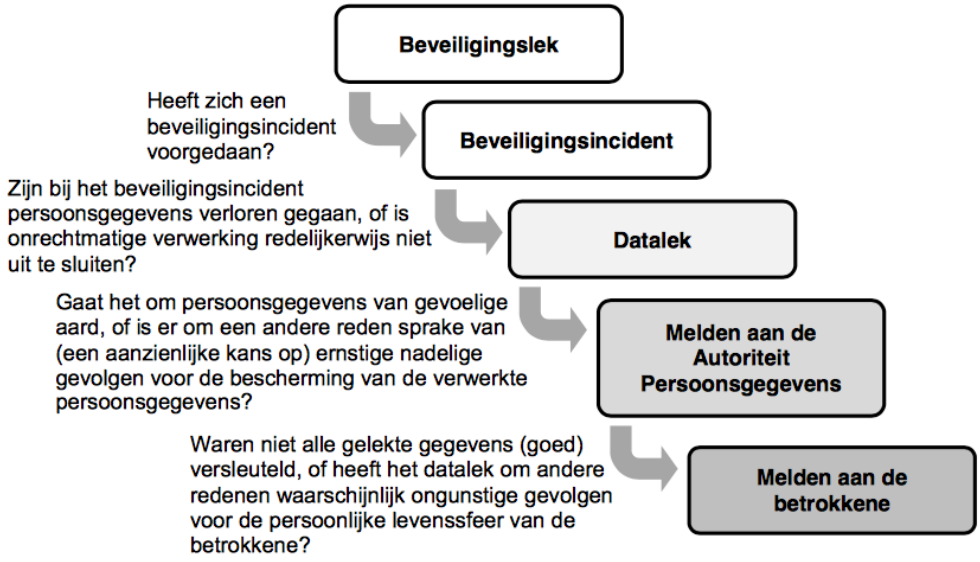
Rechten, plichten en verwerkovereenkomsten
Betrokkenen krijgen meer rechten onder de AVG om te controleren wat er gebeurt met hun gegevens. Een moeder van een kind in de opvang heeft het recht langs te komen en het dossier van haar kind in te zien. Een werknemer mag een kopie van zijn of haar personeelsdossier opvragen. Een persoon mag ook vragen zaken uit het dossier te wissen, dan wel aan te vullen indien de verwerking plaatsvindt op basis van onvolledige gegevens. Daarnaast hebben personen recht om – onder bepaalde omstandigheden- vergeten te worden. Dat betekent totale verwijdering van de gegevens.
Daarnaast moet een werkgever alle gegevens kant en klaar kunnen aanleveren. Stel dat een ouder naar een ander kinderdagverblijf wil, dan moet jouw organisatie een kant en klaar bestandje met alle verzamelde gegevens aanleveren dat aan de volgende organisatie gegeven kan worden.
Een aparte categorie onder de AVG zijn de zogenaamde Verwerkersovereenkomsten; contracten met leveranciers die gegevens verwerken. Bijvoorbeeld een externe salarisadministratie of een ICT-bedrijf. Aan deze verwerkingsovereenkomst worden onder de AVG zwaardere eisen gesteld. In deze contracten moeten een aantal zaken worden vastgelegd met het oog op privacy. Bijvoorbeeld wat er gebeurt met de gegevens als jullie uit elkaar gaan. Worden deze wel vernietigd na de overdacht? Maar bijvoorbeeld ook zaken als geheimhouding en dat de verwerker de gegevens niet voor eigen doeleinden mag gebruiken. Een ander erg belangrijk aspect is dat een externe partner ook aantoont passende beveiligingsmaatregelen voor de gegevens te hebben. Hiervoor zijn modelovereenkomsten beschikbaar bij de overheid, afhankelijk van de dienst.

Datalekken
Veilig verwerken van persoonsgegevens valt of staat met een adequate beveiliging van het systeem. Hiervoor zijn er twee nieuwe begrippen geïntroduceerd: *Privacy by Design* en *Privacy by Default*.

Die eerste richt zich op ICT'ers. Al bij het ontwikkelen en aanschaffen van de software moet er rekening gehouden worden met het waarborgen van de privacy. Dan heb je het over software waarbij het bijvoorbeeld niet mogelijk is dat de baliemedewerker toegang heeft tot dezelfde informatie als de pedagogisch medewerker. En met *Privacy by Default* gaat het erom dat die veiligheid in de praktijk werkt. Als organisatie moet je maatregelen nemen om ervoor te zorgen dat alleen persoonsgegeven verwerkt worden die noodzakelijk zijn voor het specifieke doel dat je wilt bereiken. Je mag als bedrijf bijvoorbeeld niet meer automatisch iemand een nieuwsbrief aansmeren als hij iets koopt, maar moet daar apart toestemming voor vragen.
Mocht er nou toch iets misgaan -een laptop met gevoelige informatie die in de trein is blijven liggen, een mail met salarissen die per ongeluk naar de verkeerde (externe) personen is gestuurd of het systeem wordt gehackt- dan spreek je van een datalek.
Bij een datalek is er onbedoeld inbreuk op de beveiliging van persoonsgegevens gemaakt. Onder een datalek valt niet alleen het vrijkomen (lekken) van gegevens, maar ook onrechtmatige verwerking van gegevens. Heeft dit ernstige nadelige gevolgen voor de bescherming van persoonsgegevens? Dan moet de lek gemeld worden bij het AP. En in sommige gevallen ook aan de betrokkenen.
Stel, de salarisadministratie stuurt per ongeluk een loonstrook aan de verkeerde medewerker. Dit moet absoluut gemeld worden aangezien er op deze loonstrook gegevens staan waarmee bijvoorbeeld verzekeringen kunnen worden afgesloten. Een ander voorbeeld is wanneer een medewerker op een dubieuze link heeft geklikt en het bedrijf gegijzeld is door ransomware. Ook dan moet dit gemeld worden bij de AP.
Het AP kan sancties opleggen. Zoals het ongedaan maken of rectificeren. Of je moet (tijdelijk) stoppen met het verwerken van gegevens of je krijgt een waarschuwing. Het belangrijkste is dat de AP datalekken publiceert en dat betekent dat iedereen, inclusief pers, inzage heeft. Verder worden er bij ernstige datalekken flinke boetes opgelegd.

Aan de hand van dit schema is het helder te zien wanneer je wel en wanneer niet een datalek moet melden bij de AP.

Bij de beslissing of u een gebeurtenis die zich heeft voorgedaan moet melden aan de Autoriteit Persoonsgegevens, en eventueel daarnaast ook aan de betrokkene, moet u een aantal afwegingen maken. Het onderstaande schema geeft deze afwegingen weer.



Bron: AP

Een PIA en een privacy officer

Hoe bereid je je als organisatie goed voor op de AVG? Dat kan op verschillende manieren. Bijvoorbeeld door het aanstellen van een *data protection* of *privacy officer* (dpo). Dit is een onafhankelijk iemand die zich bezig houdt met de bescherming van gegevens. Met de ingang van de AVG wordt het voor sommige bedrijven zelfs verplicht een dpo in dienst te nemen. Het gaat dan om bedrijven die zich in de kern bezighouden met het op grote schaal volgen van individuen of het verwerken van persoonsgegevens als kernactiviteit hebben en publieksinstellingen. Kinderopvang valt hier dus niet onder.
Toch is het verstandig een extern iemand naar beveiliging en opslag van gegevens te laten kijken en een Privacy Impact Assessment (PIA) te laten doen waarmee privacyrisico's van een project in een vroeg stadium op een gestructureerde en heldere manier in beeld worden gebracht. Deze PIA geldt als 0-meting en is in sommige gevallen onder de AGV verplicht. Hiervoor zijn tien criteria https://www.autoriteitpersoonsgegevens.nl/nl/onderwerpen/europese-privacywetgeving/data-protection-impact-assessment-dpia opgesteld en aan hoe meer criteria je als organisatie voldoet, hoe hoger de kans is dat je een verplichte *data protection impact assessment* moet uitvoeren.

Tip

Een helder overzicht met 10 stappen hoe je je als organisatie goed voorbereidt op de AVG, vind je hier https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/in_10_stappen_voorbereid_op_de_avg.pdf

Verzekering tegen cybercrime
De middag wordt afgesloten met een lezing (en waarschuwing) van verzekeringsexpert Roger Losekoot van de RST groep die de zaken meteen op scherp zet. “Voor zowel grote bedrijven als kleinere organisaties brengt het digitaal verwerken van persoonsgegevens grote risico’s met zich mee. Tegenwoordig is het een spelletje om een bedrijf of site te hacken. Daar moet je op voorbereid zijn.
Een hackers aanval brengt namelijk, naast heel veel ongemak, een grote financiële schade met zich mee. Niet alleen vanwege herstelkosten, maar ook door stilstand; schade die je hebt omdat je niets meer kunt.”
Daarom is een cyberrisk verzekering volgens Losekoot tegenwoordig onmisbaar. “Niet alleen dekt zo’n verzekering de financiële schade, maar ook boetes van de AP. Net als de betaling van losgeld bij ransomware als het herstel niet of bijna niet mogelijk is. Daarnaast ontvangt de verzekerde hulp bij bescherming van (media)reputatieschade.”
De verzekeraars die een cyberrisk verzekering aanbieden doen vooraf een *security scan* waarbij het digitale verkeer binnen een bedrijf twee weken gemonitord wordt. En bieden daarmee niet alleen hulp achteraf bij schade, maar ook in het voortraject om de organisatie digitaal veilig te maken.
Verder wijst ook Losekoot op het belang van een duidelijk beleid op het gebied van veiligheid. Zijn tips:

- Zorg voor een veilige werkomgeving.
Hoeveel mensen hebben toegang tot het systeem met hun mobiel? En ze verliezen die mobiel? Hoe heb je dat dichtgetimmerd? Dat moet in het beleid staan.

- Zorg voor back ups en koppel cruciale data los van het internet.
Zet een back up op bijvoorbeeld een aparte computer en koppel deze los van het internet (zodat deze niet ook blokkeert wanneer het systeem ‘gegijzeld’ wordt). Dat is een protocol dat je moet inrichten.

- Gebruik een twee-traps-inlogsysteem
Er zijn verschillende apps die dit toepassen, denk aan de *google authenticator*. Maak er een protocol van.

- Mak een sluitend protocol voor mobiele telefoons.
Wie heeft waartoe toegang?

- Beperk het aantal medewerkers met toegang tot gevoelige info.

- Zorg dat security updates direct geïnstalleerd worden.
Zeker voor verzekeraars, maar ook voor jezelf moet je de meest recente updates hebben. Updates zijn er omdat er een lek geconstateerd is!

- Maak een protocol voor als er toch een aanval plaatsvindt.
Check de website van de politie met goede tips en trucs.
https://www.nomoreransom.org/nl/prevention-advice.html