AVG

VANUIT KLANTPERSPECTIEF

Met rasse schreden komt 25 mei 2018 naderbij. Nog even en dan moeten de corporaties volledig compliant zijn met de AVG. Zoals altijd blijkt de praktijk weerbarstiger, corporaties zien de AVG - en de regels die de verordening met zich meebrengt - vooral als een extra last. Maar is dat wel correct?

Uiteraard komt er een hoop bij een AVG-compliancetraject kijken. Onder meer moet er geüpdatet beleid worden uitgevoerd, moeten er soms nieuwe procedures worden geschreven en huidige worden aangepast. En dat alles conform die nieuwe regels. Maar zijn die regels wel echt (ver)nieuw(end)?

De AVG wijzigt aan de regels omtrent de bescherming van persoonsgegevens inhoudelijk weinig. Met de Wbp en de daaraan ten grondslag liggende privacy richtlijn is een groot gedeelte van de regels al vastgesteld. Deze regelgeving is echter grootschalig genegeerd, waardoor de compliance met de AVG in feite een grote inhaalslag is. Die inhaalslag is lastig, men ervaart het als een bijzondere afwijking van de eigenlijke kerntaak en het vergt in veel gevallen veel inzet en middelen van de corporatie. Het idee is echter dat na die initiële stappen het (nagenoeg) compliant zijn en blijven enkel onderhoud vergt.

Het moment waarop de uitvoering van de AVG enkel nog onderhoud vergt, betekent dat de verplichtingen daaruit, zoals de uitvoering van rechten van betrokkenen of van meet af aan rekening houden met privacy (privacy by design), net zo gewoon zijn geworden als de jaarlijkse accountantscontrole of het bij een project rekening houden met de budgettaire beperkingen.

Maar hoe kom je daar? De AVG biedt daar weinig handvatten voor, maar essentieel is om je uitgangspositie vast te stellen. Audittrail doet dat via een nulmeting. Met die meting kun je exact zien waar de gaten vallen en hoe je die leemtes moet aanpakken. Met de uitkomsten kun je dus gericht werken aan compliance met de AVG. Dat laat onverlet dat je te allen tijde maatregelen kunt nemen om algemene persoonsgegevensbescherming te verbeteren. Dit zie je terug bij meerdere organisaties, die al voor er een daadwerkelijk compliancetraject wordt uitgezet het verzamelen en vastleggen van BSN en kopieën van legitimatiebewijzen hebben beperkt of in zijn geheel niet meer vastleggen.

De beperking aan de voorkant en een goede procedure voor de bewaring en vernietiging van gegevens, maakt al een hoop goed. Je vermindert - eventueel door natuurlijk verloop - al een hoop van de verzamelde gegevens. Ben je daardoor meteen compliant? Nee natuurlijk niet, maar je gaat wel met (hopelijk!) kleine veranderingen de goede richting op. Daarnaast wordt juist met (kleine) aanpassingen het bewustzijn van de medewerkers verhoogd en wordt AVG-compliant werken onderdeel van de bestendige bedrijfscultuur. Je pakt dus niet alleen gegevensverzameling en de bewaring daarvan aan, maar tegelijkertijd maak je medewerkers bewust van persoonsgegevensbescherming. Je zet daarmee ongemerkt dus veel grotere stappen richting compliance dan je aanvankelijk zou denken. Na 25 mei 2018 kan er nog veel, alleen moet je wel beter nadenken over het waarom en hoe.

Aletta Hoogeveen
Audittrail

Audittrail
information security | privacy | quality | grc

Aletta Hoogeveen

AVG

VANUIT AAREON

Nog maar even en dan het is 25 mei 2018: de dag waarop de Algemene Verordening Gegevensbescherming (AVG) van kracht wordt en de Wet Bescherming Persoonsgegevens (Wbp) vervangt. Voor veel organisaties betekent dat werk aan de winkel. Ook Aareon is druk bezig met het nemen van de nodige maatregelen om straks 'AVG-compliant' te zijn. Wij willen u graag op de hoogte houden van onze voortgang.

ISO27001

We zijn sinds begin 2018 ISO27001-gecertificeerd. Dat wil zeggen dat ons ISMS (Information Security Management System) voldoet aan de internationale norm en ons proces voor informatiebeveiliging in het algemeen op orde is. Onze Security Officer houdt het informatiebeveiligingsbeleid in stand.

MELDPLICHT DATALEKKEN

We hanteren een meldplicht datalekken. Als Aareon een datalek ontdekt waarbij klantgegevens betrokken zijn, dan wordt de klant altijd zo gauw mogelijk geïnformeerd zodat deze nog voldoende tijd heeft het AP en eventueel de betrokkenen op tijd informeren. Aareon informeert vanuit haar rol als verwerker uiteraard niet zelf het AP of betrokkenen.

VERWERKERSOVEREENKOMSTEN

Verder hebben we onze oude bewerkersovereen-komst aangepast tot een verwerkersovereenkomst die voldoet aan de eisen uit de AVG. Een aantal klanten heeft deze al getekend en Aareon is bezig om met al haar klanten contact op te nemen om de verwerkersovereenkomst te laten tekenen.

VFU'S (VERZOEK FUNCTIONELE UITBREIDING)

In onze software willen we een aantal functionaliteiten implementeren om de rechten van betrokkenen goed te kunnen waarborgen. Het gaat om rechten zoals het inzagerecht, het recht om vergeten te worden en privacy by design. Onze ontwikkelaars zijn hier druk mee bezig. Hieronder een greep uit de aanpassingen die eraan zitten te komen:

- De beveiliging van koppelvlakken wordt waar nodig aangescherpt.
- Er mag niet met werkelijke persoonsgegevens worden getest. Aareon biedt hiervoor ondersteuning.
- Voor het recht op inzage komt een standaard template beschikbaar om gegevens van een huurder op verzoek te kunnen verstrekken.
- Het recht op verwijdering wordt in de software mogelijk gemaakt door anonimiseren.
- Diverse overbodige velden worden uit de schermen verwijderd.
- Een verplicht strikter wachtwoordbeleid wordt in de software ingebouwd. Er komt bijvoorbeeld een standaard sjabloon met een overzicht van geregistreerde gegevens van een betrokkene dat uitgebreid kan worden door de klant. Verder worden uit Tobias AX diverse overbodige velden verwijderd. Waar nodig worden koppelvlakken voldoende beveiligd.

Voor bewaartermijnen geldt dat Aareon uitzoekt op welke manier hiermee gewerkt kan worden. Dit staat in verband met het kunnen verwijderen van gegevens uit Tobias AX. Voor nu moet dit dus procedureel binnen de woningcorporatie worden opgelost.

Aareon hoopt dat we samen met onze klanten toe kunnen werken naar een soepele overgang van Wbp naar AVG!