BELEID INFORMATIEBEVEILIGING

Vastgesteld door het Bestuur d.d.: 12 april 2018

Inhoudsopgave

1. Achtergrond
2. Eindverantwoordelijkheid
3. Doelstelling en doelgroep
4. Betrokkenen
5. Opzet informatiebeveiliging
6. Beleidsuitgangspunten
7. Verwerkingen van persoonsgegevens door Beter Wonen
8. Bewaartermijnen

1. Achtergrond

Het bestuur van Beter Wonen onderkent dat het toenemende gebruik van datacommunicatiemogelijkheden (internet, E-commerce), de complexiteit van en verwevenheid tussen geautomatiseerde systemen, de massaliteit van de dagelijkse communicatie, de omvang van de bestanden alsmede de toenemende professionalisering van de computercriminaliteit leiden tot een grote afhankelijkheid en kwetsbaarheid van de geautomatiseerde informatievoorziening binnen Beter Wonen. De risico's die hiermee samenhangen zijn zeer aanzienlijk en kunnen een bedreiging vormen voor de vertrouwelijkheid, integriteit en continuïteit van de geautomatiseerde informatievoorziening en daarmee indirect voor het imago en dus de continuïteit van Beter Wonen.

2. Eindverantwoordelijkheid

Gelet op de mogelijke impact van verstoringen op de continuïteit van Beter Wonen berust eindverantwoordelijkheid voor het beleid inzake de beveiliging en de interne controle van de informatievoorziening bij het dagelijks bestuur van Beter Wonen.

3. Doelstelling en doelgroep

De doelstelling inzake de vertrouwelijkheid, integriteit en continuïteit van de informatievoorziening van Beter Wonen luidt:

"Het bieden van een raamwerk van beleidsuitgangspunten met betrekking tot de exclusiviteit, integriteit en beschikbaarheid van de informatievoorziening, waarbinnen een evenwichtig (doeltreffend en doelmatig) stelsel van onderling samenhangende maatregelen ontwikkeld wordt, teneinde de geautomatiseerde informatievoorziening te beschermen tegen interne en externe bedreigingen."

De leden van het dagelijks bestuur dienen ervoor zorg te dragen, dat aan de in de geformuleerde beleidsuitgangspunten wordt voldaan bij de inrichting van de organisatie, procedures, werkwijze en de daarbij gehanteerde informatiesystemen.

4. Betrokkenen

a. Beveiligingsorganisatie.
b. De gebruiksorganisatie is en blijft, als houder, eindverantwoordelijke voor de door haar gebruikte informatiesystemen.
c. De systeemontwikkelingsorganisatie is verantwoordelijk voor het realiseren van de overeen te komen gewenste functionele specificaties tijdens systeemontwikkelings-trajecten.

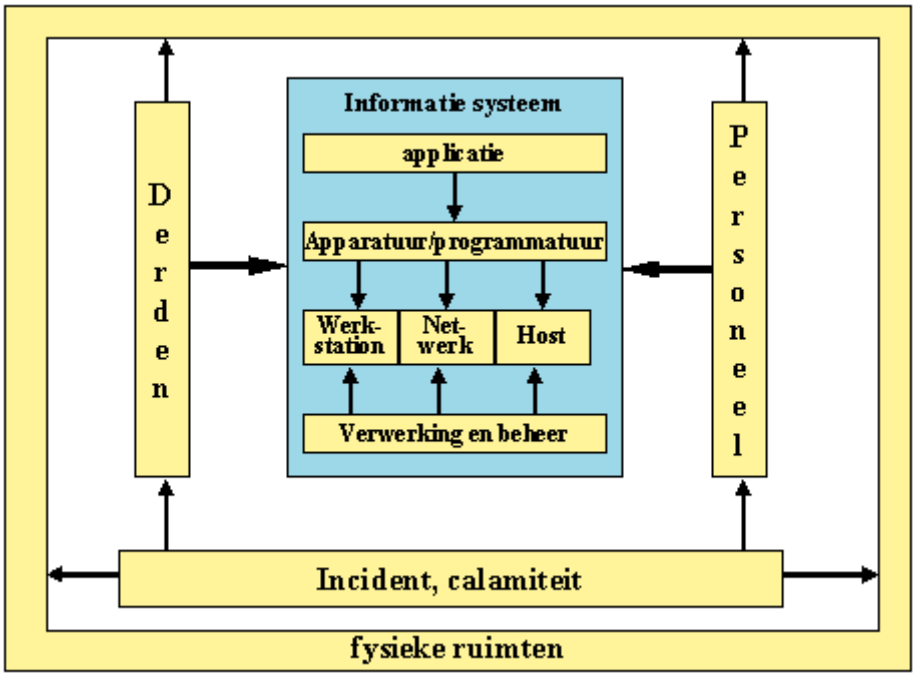
De verwerkingsorganisatie is de houder van de overeengekomen technische infrastructuur, waaronder inbegrepen de infrastructurele beveiligingsmiddelen.

5. Opzet informatiebeveiliging

Van elk (geautomatiseerd) informatiesysteem, inclusief de daarbij behorende gegevens, zijn de leden van het dagelijks bestuur expliciet als houder benoemd. Het houderschap impliceert de eindverantwoordelijkheid voor het betreffende systeem, inclusief het bepalen van bij het systeem te onderkennen risico's, het classificeren van het systeem en de daarbij behorende gegevens en het (laten) ontwikkelen van adequate beveiligingsmiddelen en interne controlemaatregelen. Naast de applicatie betreft dit ook de juiste inzet van de infrastructurele

componenten (werkstations, servers en LAN/WAN), de juiste verwerking, het adequate beheer, het goed functioneren van het personeel, het maken van afspraken met derden, fysieke beveiliging en voorzieningen om incidenten en calamiteiten te voorkomen of af te handelen.

In onderstaand figuur zijn alle genoemde deelgebieden van een informatiesysteem opgenomen.



Figuur 1: aandachtsgebieden security

Er wordt gesproken over eindverantwoordelijk omdat een aantal aspecten van het informatiesysteem uitbesteed worden aan andere houders. Dit kan zowel betrekking hebben op aspecten tijdens de ontwikkeling van het systeem, als tijdens het beheer, het gebruik en/of bepaalde deelcomponenten van het totale systeem.

De te treffen maatregelen, alsmede de prioriteitsstelling hierin, dienen te worden bepaald op grond van een op te stellen risicoanalyse, waarin: de bedreigingen tegen een betrouwbare en op continuïteit gerichte, (geautomatiseerde) informatievoorziening en de daarmee samenhangende risico's worden onderkend en een evenwichtig stelsel van onderling samenhangende maatregelen wordt ontwikkeld ter reducering van de risico's tegen acceptabele kosten.

Hierbij wordt derhalve niet een maximaal beveiligingsniveau nagestreefd, maar een optimaal niveau. Bij het uitvoeren van de risicoanalyse wordt Beter Wonen ondersteund door OMNIS-it. Zij vervult in deze een coördinerende rol, opdat overlappingen en tekortkomingen in het totale stelsel van maatregelen binnen Beter Wonen worden voorkomen.

6. Beleidsuitgangspunten

a. De fysieke en logistieke beveiliging van de computercentra en het kantoor van Beter Wonen is zodanig, dat de vertrouwelijkheid, integriteit en beschikbaarheid van de gegevens en gegevensverwerking gewaarborgd zijn.

b. Aanschaf, installatie en onderhoud van geautomatiseerde gegevensverwerkende systemen, alsmede inpassing van nieuwe technologieën, mogen geen afbreuk doen aan het niveau van veiligheid van de totale informatievoorziening.
c. Het personeelsbeleid is mede gericht op het leveren van een bijdrage aan de vertrouwelijkheid, integriteit en continuïteit van de informatievoorziening.
d. Opdrachten aan derden voor het uitvoeren van werkzaamheden worden zodanig omgeven met maatregelen, dat er geen inbreuk op de vertrouwelijkheid, integriteit en continuïteit van de informatievoorziening kan ontstaan.
e. Bij de verwerking en het gebruik van gegevens worden maatregelen getroffen om de privacy van klanten en personeel te waarborgen.
f. Logische toegangsbeveiliging zorgt ervoor, dat ongeautoriseerde personen of processen geen toegang krijgen tot de geautomatiseerde systemen, gegevensbestanden en programmatuur van Beter Wonen.
g. Gegevensverstrekking intern en extern gebeurt op basis van ‘need to know’. Er worden maatregelen getroffen om te voorkomen dat informatie in handen van personen terechtkomt, die deze informatie niet strikt nodig hebben. Ook de toegang tot informatiesystemen wordt volgens dit principe adequaat beveiligd. Voor ICT-beheerders wordt hierop een uitzondering gemaakt, om te komen tot een betere service aan de gebruikers.
h. Datatransport is zodanig met beveiligingsmaatregelen omkleed, dat geen inbreuk kan worden gepleegd op de vertrouwelijkheid en de integriteit van de gegevens en op de informatievoorziening als geheel.
i. Teneinde computervirusinfecties te voorkomen wordt er slechts gewerkt met geautoriseerde versies van (legale) programmatuur.
j. Het beheer en de opslag van gegevens zijn zodanig, dat geen informatie verloren kan gaan.
k. Incidenten worden adequaat afgehandeld en hier worden ‘lessons learned’ uitgetrokken.
l. Er zijn calamiteitenvoorzieningen om de continuïteit van de bedrijfsvoering en de informatievoorziening te waarborgen en imagoschade te voorkomen.

7. Verwerkingen van persoonsgegevens door Beter Wonen

7.1 Toegestane doeleinden verwerking

De verwerking mag alleen geschieden voor:
a. het uitvoeren van de huurovereenkomst;
b. het uitvoeren van een arbeids- of dienstverleningsovereenkomst;
c. werving en selectie van personeel en leden Raad van Commissarissen en bestuur;
d. het berekenen en vastleggen van inkomsten en uitgaven;
e. het doen van betalingen;
f. het innen van vorderingen (inclusief het in handen van derden stellen van die vorderingen);
g. het onderhoud en de reparatie van de te huren en verhuren roerende en onroerende zaken;
h. het behandelen van geschillen;
i. het doen uitoefenen van accountantscontrole;
j. activiteiten van intern beheer.

7.2 Toegestane (categorieën) verwerkte gegevens

Alleen de volgende persoonsgegevens mogen worden verwerkt:
a. NAW-gegevens;
b. BSN (personeel en leden RvC en bestuur);
c. geboortedatum;
d. burgerlijke staat;
e. telefoonnummer;
f. mailadres;
g. bankrekeningnummer;
h. kopie legitimatiebewijs;
i. verklaring inkomen;
j. Woongaardnummer.

7.3 Toegestane (categorieën) ontvangers van de gegevens

De persoonsgegevens mogen alleen worden verstrekt aan degenen, inclusief derden, die:
a. belast zijn met de hierboven onder 1. opgesomde werkzaamheden, of
b. leiding geven aan de hierboven onder 1. opgesomde werkzaamheden, of
c. noodzakelijk zijn betrokken bij de hierboven onder 1. opgesomde werkzaamheden.

7.4 Criteria duur opslag persoonsgegevens

Bij het bepalen van de bewaartermijn wordt rekening gehouden met de volgende factoren:
a. het doel/de doelen waarvoor de persoonsgegevens verzameld zijn (de noodzaak om de gegevens voor dat doel te bewaren);
b. wettelijke bewaartermijnen.

7.5 Recht op inzage, rectificatie, ontvangen of wissen van de persoonsgegevens

Betrokkene heeft het recht op inzage, rectificatie, ontvangen of wissen van de persoonsgevens. Hiervoor kan contact worden opgenomen met de functionaris

gegevensbescherming van Beter Wonen, de heer mr. M.C. van Es, via (0184) 68 22 44 of mvanes@beterwonenstreefkerk.nl.

7.6 Meldplicht datalek

Wanneer verhuurder een datalek constateert, zal hiervan onverwijld melding worden gedaan bij de Autoriteit Persoonsgegeven en de betrokkene(n).

7.7 Recht om een klacht in te dienen bij de Autoriteit Persoonsgegevens

Betrokkene kan een klacht indienen bij de Autoriteit Persoonsgegevens.

8. Bewaartermijnen

8.1 Inleiding

Als hoofdregel geldt dat persoonsgegevens niet langer mogen worden bewaard dan noodzakelijk. De bepaling van bewaartermijnen geschiedt op meerdere manieren, waar in dit hoofdstuk nader zal worden ingegaan.

8.2 Wettelijke bewaartermijnen

Fiscale bewaartermijnen/boekhouding: 7 jaar (art. 52 lid 4 AWR)
De basisgegevens van de fiscale administratie dienen 7 jaar bewaard te blijven. Dit zijn onder meer:

- het grootboek;
- de debiteuren- en crediteurenadministratie;
- de loonadministratie.

Loonadministratie: 7 jaar: basisgegevens van de loonadministratie zoals informatie over salaris, arbeidsvoorwaarden en andere fiscale gegevens.

Loonbelastingverklaring: 5 jaar na het einde van het kalenderjaar waarin de dienstbetrekking is geëindigd (art. 12.1 lid 5 uitvoeringsregeling LB 2011).

Kopie identiteitsbewijs van werknemers: 5 jaar na het einde van het kalenderjaar waarin de dienstbetrekking is geëindigd (art. 7.5 lid 4 uitvoeringsregeling LB 2011)

Kopieën van beschikkingen of verklaringen die van de werknemer zijn ontvangen: 5 jaar na het einde van het kalenderjaar waarin de dienstbetrekking is geëindigd.

8.3 Aansluiting bij het vrijstellingsbesluit Wbp

Onder de huidige Wet bescherming persoonsgegevens zijn er in het vrijstellingsbesluit Wbp bewaartermijnen opgenomen die niet mogen worden overschreden om binnen het vrijstellingsbesluit te vallen. Dit vrijstellingsbesluit vervalt onder de Algemene Verordening Gegevensbescherming en deze termijnen gaan geen harde grenzen vormen. Voor Beter Wonen zijn deze termijnen wel een indicatie wat als een redelijke bewaartermijn (maximaal) wordt gezien, waarbij wordt aangesloten bij de wettelijke regel (AVG): ‘niet langer bewaren dan noodzakelijk’.

Sollicitatie: 4 weken na het einde van de sollicitatieprocedure of met toestemming van de sollicitant maximaal 1 jaar na beëindiging van de sollicitatieprocedure.

Ziekte: Afgeronde ziekteverzuimperioden of gesloten re-integratiedossiers worden in beginsel na 2 jaar uit het personeelsdossier verwijderd.

Arbeidsconflict: Soms is het nodig om een personeelsdossier langer te bewaren door bijvoorbeeld een arbeidsconflict.

Intern beheer zoals planningen, interne telefoon- en adressenlijsten: 6 maanden nadat de persoon uit dienst is/geen werkzaamheden meer verricht.

Personeelsadministratie: 2 jaar na einde dienstverband.

Loonadministratie: 7 jaar na einde dienstverband (tenzij en voor zover een wettelijke bewaarplicht geldt).

Andere personeelsgegevens: Voor andere gegevens uit het personeelsdossier is de richtlijn: 2 jaar nadat de werknemer uit dienst is. Met uitzondering van de kopie ID werknemers: 5 jaar na einde dienstverband.

Loonbeslagen: tot moment van opheffing.

Gegevens met betrekking tot toegangscontrole: 6 maanden na einde dienstverband.

Gegevens van leveranciers van goederen en diensten: 2 jaar na afname.

Communicatie bestanden/adressenlijsten/mailinglijsten: 1 jaar nadat de relatie tussen de betrokkene en de verantwoordelijke is verbroken.

Klachten: 2 jaar na afhandeling van de klacht.

Juridische procedures: 2 jaar na afhandeling van de procedure.

Gegevens huurders: 2 jaar na het einde van de huur.

Leden: 2 jaar nadat het lidmaatschap is beëindigd.

Oud-ledengegevens: Er geldt geen termijn. Dit is een archief. De persoonsgegevens moeten worden verwijderd op verzoek van het oud-lid of bij diens overlijden.

Debiteuren en crediteuren: 2 jaar nadat de vordering is voldaan.

Het bestuur van Beter Wonen Streefkerk,

M.C. van Es, voorzitter

E. Noorland-Hardeman, secretaris/penningmeester

R.C. de Bruijn, 2e secretaris

R. Vos, 2e penningmeester