Protocol meldplicht datalekken

Disclaimer
Dit protocol is geen juridisch document of advies en beoogt niet volledig te zijn, maar geeft slechts een indicatie van bepaalde AVG verplichtingen. VGM NL is niet aansprakelijk voor enige schade op welke wijze dan ook voortvloeiende uit (het gebruik van) verstrekte informatie.

VASTGOED MANAGEMENT NEDERLAND

sinds 1933
van der BORDEN
vastgoedprofessionals

1. Inleiding

Per 25 mei 2018 geldt ingevolge de Algemene Verordening Gegevensbescherming ("AVG") een meldplicht datalekken. Om aan de verplichtingen uit deze wet te voldoen heeft "Van der Borden Vastgoedprofessionals" voor al haar bedrijfsonderdelen *(te weten: Woningmakelaardij, Bedrijfsmakelaardij, Huur & Beheer en VVE-Beheer*) dit protocol vastgesteld.

Volgens de AVG dient de Autoriteit Persoonsgegevens ("AP" direct, uiterlijk binnen 72 uur, in kennis te worden gesteld van een 'inbreuk op de beveiliging van persoonsgegevens' die 'leidt tot de aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens'. In dit protocol wordt een dergelijk incident aangeduid als een "Datalek".

De betrokkene (de persoon op wie de gegevens betrekking hebben) dient daarnaast onverwijld in kennis te worden gesteld van de inbreuk indien de inbreuk 'een groot risico voor de rechten en vrijheden van de betrokkene met zich meebrengt'.

Aan de beantwoording van de vraag moet een zorgvuldige (belangen)afweging voorafgaan. Hierbij is bijvoorbeeld de aard en de omvang van de persoonsgegevens die gelekt zijn van belang. Als er bijzondere persoonsgegevens, zoals gegevens over gezondheid, gelekt zijn, dan is de melding meestal noodzakelijk.

De AVG stelt zware sancties op overtreding van de meldplicht. Het is daarom van belang dat dit protocol strikt wordt nageleefd.

De heer Peter Zee, (hierna: "de Contactpersoon") draagt binnen Van der Borden als Procesmanager AVG zorg voor de naleving van de meldplicht. Het is in geval van mogelijke Datalekken van belang de Contactpersoon direct te informeren, zodat de Contactpersoon de situatie kan beoordelen en de nodige acties in gang kan zetten.

2. Wanneer kan er een meldplicht zijn

Er is sprake van een datalek als er een inbreuk in verband met persoonsgegevens heeft plaatsgevonden. Alleen een dreiging of een tekortkoming in de beveiliging is niet voldoende; er moeten daadwerkelijk persoonsgegevens gelekt zijn.

Onder een datalek verstaat de AP persoonsgegevens die gelekt of vernietigd zijn als gevolg van een beveiligingsincident. Bij het lek zijn persoonsgegevens blootgesteld aan verlies of onrechtmatige verwerking. Bij verlies zijn de persoonsgegevens er niet meer. Onder onrechtmatige verwerking vallen bijvoorbeeld onbevoegde kennisneming, wijziging, aantasting of de verstrekking daarvan.

Voorbeelden van inbreuken in verband met persoonsgegevens kunnen zijn:
- kwijtraken van een USB -stick
- diefstal van een laptop
- inbraak door een hacker

- persoonsgegevens per ongeluk gepubliceerd
- hacking, mailware of fishing

- persoonsgegevens aan verkeerde persoon verstuurd
- calamiteiten zoals brand in een datacentrum

Ga er bij twijfel van uit dat sprake is van een Datalek zodat er een (interne) melding moet worden gedaan.

3. Ieder mogelijk Datalek direct intern melden

Ieder Datalek dient direct en met hoge prioriteit gemeld te worden aan de Contactpersoon.
Voorzie de Contactpersoon van zoveel mogelijk relevante gegevens, zoals een korte beschrijving van wat er is gebeurd, datum en tijdstip, een schatting van het aantal betrokken natuurlijke personen, soorten gegevens, en mogelijke gevolgen voor de betrokken personen. Dit kan later overigens worden aangevuld, vanwege de korte termijnen is het van belang om vooral te zorgen dat de Contactpersoon snel op de hoogte is. Controleer of de Contactpersoon ook daadwerkelijk van de e-mail kennis heeft genomen. Bij afwezigheid van de Contactpersoon dient mede contact te worden gezocht met de leidinggevende van de afdeling.

Wat gebeurt er met de interne melding

STAPPENPLAN DATALEKKEN

Processtappen	Activiteit	Verantwoordelijke persoon
1. Er wordt een (mogelijk) datalek ontdekt	- Maak direct intern melding van (mogelijke) datalek - Informeer de verantwoordelijke Contactpersoon	Medewerker die het ontdekt
2. Beoordeel het datalek	- Onderzoek het beveiligingsincident - Onderzoek of er persoonsgegevens verloren zijn gegaan of onrechtmatig gebruikt kunnen worden - Beoordeel wie of welke afdelingen binnen de organisatie hierbij betrokken zijn - Beoordeel of er een verwerker betrokken is bij het incident. Zo ja dan dient deze bij het proces betrokken te worden	Manager van afdeling waar binnen het datalek heeft plaatsgebonden Manager van de afdeling die verantwoordelijk is voor de beveiligingsincidenten (bijvoorbeeld IT) Aangewezen contactpersoon
3. Bestrijdt het datalek	- Stop het datalek als het nog kan - Neem andere maatregelen om het datalek en de daaruit voortvloeiende schade te beperkten - Leg de acties van de genomen maatregelen vast in het dossier	Manager van afdeling waar binnen het datalek heeft plaatsgebonden Manager van de afdeling die verantwoordelijk is voor de beveiligingsincidenten (bijvoorbeeld IT) Aangewezen contactpersoon

4.Vaststellen impact datalek	- Onderzoek het datalek en de gevolgen daarvan - Onderzoek de aard van de gegevens die gelekt zijn. Bijv. gezondheidsgegevens, wachtwoorden, gegevens over financiële situatie of die kunnen leiden tot stigmatisering/ misbruik - Onderzoek de omvang van de gelekte gegevens - Beoordeel welke impact het lek kan hebben op de betrokken personen - Stel vast wat de nadelige gevolgen kunnen zijn	Manager van afdeling waar binnen het datalek heeft plaatsgebonden Manager van de afdeling die verantwoordelijk is voor de beveiligingsincidenten (bijvoorbeeld IT) Aangewezen contactpersoon

5.Vaststellen Meld- en Herstelaanpak	- Bepaal aanpak/informeren AP - Bepaal aanpak/informeren betrokkenen - Bepaal acties voor nazorg betrokkenen - Bepaal acties voor belang van de organisatie - Bepaal acties voor verbetering beveiliging	Manager van afdeling waar binnen het datalek heeft plaatsgebonden Manager van de afdeling die verantwoordelijk is voor de beveiligingsincidenten (bijvoorbeeld IT) Aangewezen contactpersoon
6. Melden AP*	- Indien besloten wordt om AP te informeren dan moet dat binnen 72 uur - Melding via de website van het AP - Van tevoren kan het Meldformulier Datalekken gebruikt worden (Bijlage 1)	Aangewezen contactpersoon Functionaris Gegevensbescherming Bestuur
7. Melden betrokkenen**	- Melding via bijvoorbeeld brief - Meedelen wat er is gebeurd, welke persoonsgegevens getroffen zijn en wat de mogelijke gevolgen van het datalek kunnen zijn. - Informeren over de maatregelen die de organisatie neemt en die de betrokkene zelf kan nemen om schade te voorkomen	Aangewezen contactpersoon Bestuur Marketing/communicatie
8.Uitvoeren herstelwerkzaamheden	- Herstel het datalek - Verbeteren van de beveiliging - Lever nazorg aan de betrokkenen	Manager van de afdeling die verantwoordelijk is voor de beveiligingsincidenten (bijvoorbeeld IT) Aangewezen contactpersoon
9. Optimaliseer het beveiligings- en het Datalek proces	- Registreer, evalueer en verbeter de beveiliging en het proces inzake melding datalekken	Aangewezen contactpersoon Bestuur Manager van de afdeling die verantwoordelijk is voor de beveiligingsincidenten (bijvoorbeeld IT)

* *Melding aan de Autoriteit Persoonsgegevens kan alleen achterwege blijven indien het onwaarschijnlijk is dat het datalek leidt tot een hoog risico voor de rechten en vrijheden van de betrokkenen. Of hiervan sprake is hangt mede af van de aard en omvang van de gelekte persoonsgegevens. Indien bijvoorbeeld uitsluitend de adresgegevens zijn gelekt*

van een kleine groep betrokkenen, dan is het onwaarschijnlijk dat er sprake is van een hoog risico. Dat is wellicht anders indien de adresgegevens in combinatie met het lidmaatschap van de patiënten of cliëntenorganisatie zijn gelekt. Het lidmaatschap van de organisatie kan gezien worden als een gevoelig gegeven en de leden van de organisatie kunnen wellicht behoren tot een kwetsbare groep, die extra bescherming

* *nodig heeft. Bij de afweging van het risico voor de rechten en vrijheden van de betrokken zal altijd de Functionaris Gegevensbescherming betrokken moeten worden.*

** *Indien het datalek waarschijnlijk een groot risico voor de rechten en vrijheden van de betrokkenen veroorzaakt, moet het datalek ook aan de betrokkenen gemeld worden. Het risico zal bijvoorbeeld moeten worden beoordeeld aan de hand van de aard en de hoeveelheid van de gelekte gegevens. Als er persoonsgegevens van gevoelige aard (bijv. gezondheidsgegevens) gelekt zijn, zal het lek in ieder geval gemeld moeten worden aan de betrokkenen. Bij de afweging van het risico voor de rechten en vrijheden van de betrokkenen zal altijd de Functionaris Gegevensbescherming betrokken moeten worden.*

4. Overeenkomsten met verwerkers

Indien onze organisatie een derde inschakelt om in opdracht persoonsgegevens te verwerken (“verwerker”), blijft Van der Borden verantwoordelijk voor de naleving van de verplichtingen uit de AVG. Dit dient te worden vastgelegd in een schriftelijke overeenkomst, de verwerkersovereenkomst. Met het oog op de Meldplicht Datalekken dient de verwerkersovereenkomst vanaf 25 mei 2018 onder meer een regeling te bevatten over de wijze waarop aan de meldplicht Datalekken wordt voldaan. Alle verwerkersovereen-komsten moeten worden gesloten volgens het meest actuele model dat Van der Borden hiervoor hanteert. Eventuele verwerkersovereenkomsten die nog niet voldoen aan de per 25 mei 2018 geldende standaarden, moeten worden aangepast.

5. Vragen

Voor vragen over de meldplicht Datalekken kun je contact opnemen met de heer P. Zee, Procesmanager AVG.

E-mail: pzee@vanderborden.nl
Tel: 072-5141000 / 072-5181800 / 072-5181828

Bijlage 1. Formulier Melding datalek

In dit formulier zijn de gegevens opgenomen die gemeld moeten worden aan de Autoriteit Persoonsgegevens indien er sprake is van een datalek.

Nieuwe of bestaande melding

1. Gaat het om een nieuwe of een bestaande melding? (kies een van de opties)

   ☐ Nieuw
   ☐ Bestaand

2. Indien bestaand:

   Wat is het nummer van de oorspronkelijke melding? Klik of tik om tekst in te voeren.

   Wat is de strekking van de vervolgmelding? (kies een van de opties)

   ☐ Toevoegen of wijzigen van informatie betreffende de eerdere melding
   ☐ In trekking van de eerdere melding

   Wat is de reden van intrekking? Klik of tik om tekst in te voeren.

Wettelijk kader voor de melding

3. Op grond van welke wettelijke bepaling doet u de melding?

   ☐ artikel 33 AVG
   ☐ artikel 11.3a, eerste lid, van de Telecommunicatiewet

Algemene informatie en contactpersoon

4. Over welk bedrijf of welke organisatie gaat het?

   a. Naam van het bedrijf of de organisatie
   b. (Bezoek)adres
   c. Postcode
   d. Plaats
   e. KvK-nummer

5. Wie heeft het datalek gemeld?

   a. Naam van de persoon
   b. Functie van de persoon
   c. E-mailadres van de persoon
   d. Telefoonnummer van de persoon
   e. Alternatief telefoonnummer

6. Met wie kan de Autoriteit Persoonsgegevens contact opnemen voor nadere informatie over de melding?

De melder is de contactpersoon. Anders:

a. Naam contactpersoon
b. Functie van de contactpersoon
c. E-mailadres van de contactpersoon
d. Telefoonnummer van de contactpersoon
e. Alternatief telefoonnummer van de contactpersoon

Gegevens over het datalek

7. Wat is de aard van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest, bijvoorbeeld:

   ☐ USB stick of laptop is gestolen
   ☐ Functie van de contactpersoon
   ☐ Hacking, malware of fishing
   ☐ Persoonsgegevens van het verkeerde lid gepubliceerd in het ledenportal
   ☐ Persoonsgegevens van het verkeerde lid aan verkeerde ontvanger

8. Geef een samenvatting van het incident waarbij de inbreuk op de beveiliging van persoonsgegevens zich heeft voorgedaan. Klik of tik om tekst in te voeren.

9. Vond de inbreuk plaats in een verwerking die is uitbesteed aan een andere organisatie? Zo ja, aan welke organisatie/verwerker: Klik of tik om tekst in te voeren.

10. Van hoeveel personen zijn persoonsgegevens betrokken bij de inbreuk?

    a. Minimaal: Klik of tik om tekst in te voeren.
    b. Maximaal: Klik of tik om tekst in te voeren.

11. Omschrijf de groep mensen van wie persoonsgegevens zijn betrokken bij de inbreuk. Klik of tik om tekst in te voeren.

12. Wanneer vond de inbreuk plaats?

    ☐ Op (datum)
    ☐ Tussen (begindatum periode) en (einddatum periode)
    ☐ Nog niet bekend

13. Wat is de aard van de inbreuk? (selecteer één of meerdere opties)

    ☐ Lezen (vertrouwelijkheid)
    ☐ Kopiëren
    ☐ Veranderen (integriteit)
    ☐ Verwijderen of vernietigen (beschikbaarheid)
    ☐ Diefstal
    ☐ Nog niet bekend

14. Om welk type persoonsgegevens gaat het? (selecteer één of meer opties)

- ☐ Naam-, adres- en woonplaatsgegevens
- ☐ Telefoonnummers
- ☐ E-mailadressen of andere adressen voor elektronische communicatie
- ☐ Toegangs- of identificatiegegevens (bv. inlognaam/wachtwoord of klantnummer)
- ☐ Financiële gegevens (bv. rekeningnummer, creditcardnummer)
- ☐ Burgerservicenummer (BSN) of sofinummer
- ☐ Paspoortkopieën of kopieën van ander legitimatiebewijzen
- ☐ Geslacht, geboortedatum en/of leef
- ☐ Hacking, malware of fishing
- ☐ Bijzondere persoonsgegevens (bv. over iemands gezondheid)
- ☐ Overige gegevens, namelijk: (vul aan)

15. Welke gevolgen kan de inbreuk hebben voor de persoonlijke levenssfeer van de betrokkenen? (selecteer één of meer opties)

- ☐ Stigmatisering of uitsluiting
- ☐ Schade aan de gezondheid
- ☐ Blootstelling aan (identiteits)fraude
- ☐ Bloodstelling aan spam of phishing
- ☐ Anders, namelijk: (vul aan)

Vervolgacties naar aanleiding van het datalek

16. Welke technische en organisatorische maatregelen heeft uw organisatie getroffen om de inbreuk aan te pakken en om verdere inbreuken te voorkomen? Klik of tik om tekst in te voeren.

17. Heeft u het datalek gemeld aan de betrokkenen of bent u van plan dat te gaan doen? (selecteer één of meer opties)

- ☐ Ja
- ☐ Nee
- ☐ Nog niet bekend

18. Wanneer heeft u het datalek gemeld aan de betrokkenen of wanneer gaat u dit doen?

- ☐ Ik heb het datalek aan de betrokkenen gemeld op (datum)
- ☐ Ik ga het datalek aan de betrokkenen melden op (datum)
- ☐ Nog niet bekend

19. Wat is de inhoud van de melding aan de betrokkenen? Klik of tik om tekst in te voeren.

20. Hoeveel betrokkenen heeft u in kennis gesteld of gaat u in kennis stellen? Klik of tik om tekst in te voeren.

21. Welk communicatiemiddel of welke communicatiemiddelen gebruikt u of gaat u gebruiken bij het in kennis stellen van de betrokkenen? Klik of tik om tekst in te voeren.

22. Indien u bij vraag 17 nee hebt geantwoord: waarom ziet u af van het melden van het datalek aan de betrokkenen?

☐ De technische beschermingsmaatregelen die ik heb getroffen bieden voldoende bescherming om de melding aan de betrokkene achterwege te kunnen laten
☐ Het is onwaarschijnlijk dat het datalek ongunstige gevolgen zal hebben voor de persoonlijke levenssfeer van de betrokkene, want: (verder invullen)
☐ Anders, namelijk (verder invullen)

Technische beschermingsmaatregelen

23. Waren de persoonsgegevens versleuteld, gehasht of op een andere manier onbegrijpelijk of ontoegankelijk gemaakt voor onbevoegden?

☐ Ja
☐ Nee
☐ Deels, namelijk: (vul aan)

24. Als de persoonsgegevens geheel of deels onbegrijpelijk of ontoegankelijk zijn gemaakt, op welke manier is dit dan gebeurd? Klik of tik om tekst in te voeren.

Internationale aspecten

25. Heeft de inbreuk betrekking op personen in andere EU-landen?

☐ Ja
☐ Nee
☐ Nog niet bekend

26. Heeft uw bedrijf of organisatie het datalek gemeld bij toezichthouders in een of meer andere EU-landen?

☐ Ja, namelijk: Klik of tik om tekst in te voeren.
☐ Nee

Vervolgmelding

27. Is naar uw mening deze melding compleet?

☐ Ja, de vereiste informatie is verstrekt en er is geen vervolgmelding nodig
☐ Nee, er komt later een vervolgmelding met aanvullende informatie over deze inbreuk