



Incidentenregeling

Altera Vastgoed NV

Vastgesteld in de vergadering 24 mei 2018 van het MT

Aanleiding en doel

AlterA Vastgoed N.V. (verder te noemen: Altera) ziet de goede reputatie en integriteit van haar organisatie als een belangrijk vereiste om succesvol te opereren als vastgoedbeleggingsinstelling. Ondanks alle inspanningen, kunnen calamiteiten of incidenten zich voordoen. Dit kan bij Altera zelf gebeuren, maar ook bij één van haar Opdrachtnemers. Ook in dat geval kan de reputatie van Altera in het geding komen.

Het doel van deze Incidentenregeling is om aan belanghebbenden duidelijk te maken op welke wijze Incidenten worden gemeld, vastgelegd, onderzocht en aanleiding zijn voor het nemen van corrigerende maatregelen. Doel is niet alleen de ontstane situatie te corrigeren, maar tevens te leren van de situatie die zich heeft voorgedaan.

Onderscheid tussen incident en misstand

Het Integriteitbeleid van Altera beschrijft het overkoepelend beleid van op het gebied van een beheerste en integere bedrijfsvoering. In het Integriteitbeleid is beschreven in welke afzonderlijke regelingen dit beleid verder vorm heeft gekregen. Deze Incidentenregeling is één van deze onderliggende beleidsstukken.

Een Incident is een gedraging of gebeurtenis die een ernstig gevaar vormt voor de integere uitoefening van het bedrijf van de vennootschap. Een Incident kan vele vormen aannemen, zoals een operationeel incident, een grove overtreding van wet- en regelgeving (misstand), of een beveiligingsincident. Ook andere vormen van Incidenten zijn denkbaar. De oorzaak kan zowel intern als extern gelegen zijn. Afhandeling geschiedt conform de Incidentenregeling.

Bij een misstand of onregelmatigheid is sprake van misbruik van een (machts- of kennis)positie of overtreding van (interne) regels door één of meerdere individuen. Een grove misstand kan echter tevens een incident zijn, indien deze misstand een ernstig gevaar vormt voor de integere uitoefening van het bedrijf.

Afhandeling geschiedt conform de Klokkeluidersregeling.

In geval een verbonden persoon twijfelt of sprake is van een misstand, een onregelmatigheid, dan wel van een Incident, kan hij vooraf altijd contact opnemen met de vertrouwenspersoon, om gezamenlijk de meest passende route te kiezen.

1. Definities

1.1 Incident:

Gedraging of gebeurtenis die een ernstig gevaar vormt voor de integere uitoefening van het bedrijf van Altera.

Een Incident kan vele vormen aannemen, zoals een operationeel Incident, een grove overtreding van wet- en regelgeving (misstand), of een beveiligingsincident. Ook andere vormen van Incidenten zijn denkbaar. De oorzaak kan zowel intern als extern gelegen zijn.

Een Incident kwalificeert zich als zwaar incident als er sprake is van:

- a. een ernstig gevaar voor de integere bedrijfsuitoefening van Altera;
- b. een groot afbreukrisico in de media;
- c. een belangrijke invloed op de bedrijfsvoering;
- d. de betrokkenheid van het Openbaar Ministerie;
- e. fraude;
- f. een aanwijzing van de toezichthouder, een last onder dwangsom of het voornemen om een bestuurlijke boete op te leggen.

1.2 Datalek (zie bijlage Procedure Datalekken)

Een inbreuk op de beveiliging (zoals bedoeld in artikelen 4 lid 12, 33 en 34 AVG)¹ waarbij persoonsgegevens zijn blootgesteld aan verlies of onrechtmatige verwerking; dus blootgesteld aan datgene waartegen beveiligingsmaatregelen (artikel 5 AVG) bescherming moesten bieden.

¹ "inbreuk in verband met persoonsgegevens: een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens"

- 1.3 Melder:
Eenieder die een melding doet van een Incident in het kader van deze regeling. Dit kunnen verbonden personen² zijn van Altera, maar tevens werknemers van Opdrachtnemers of andere belanghebbenden.
- 1.4 Meldpunt:
Voor datalekken is het meldpunt de Functionaris Gegevensbescherming van de vennootschap. Voor overige incidenten is dit de algemeen directeur of in het geval de melder betrokkenheid van directieleden vermoedt de voorzitter van de Raad van Commissarissen van de vennootschap of de vertrouwenspersoon.
- 1.5 Opdrachtnemer:
Iedere derde partij, zowel een natuurlijke of rechtspersoon, die (in)direct op verzoek van Altera werkzaamheden voor, namens of ten behoeve van Altera verricht. Hieronder kunnen ook Opdrachtnemers vallen die voor Altera persoonsgegevens verwerken (Verwerkers).

2. Algemeen

- 2.1 De directie van Altera is verantwoordelijk voor een tijdige en efficiënte afhandeling van Incidenten, de registratie daarvan en het nemen van passende corrigerende maatregelen.
- 2.2 De directie van de vennootschap zal ervoor zorgdragen dat de Regeling Incidenten bekend is bij alle verbonden personen van Altera en beschikbaar is voor de relevante werknemers van Opdrachtnemers of andere belanghebbenden via de Altera website.

3. Het melden van een Incident

- 3.1 Iedere verbonden persoon is verplicht een Incident, of een vermoeden daarvan, terstond te melden bij het Meldpunt. Meldingen kunnen zowel mondeling als schriftelijk plaatsvinden.
- 3.2 Andere belanghebbenden met kennis van of vermoedens omtrent een Incident, worden uitgenodigd dit terstond onder de aandacht van Altera te brengen.
- 3.3 De Melder en de externe compliance officer krijgen een schriftelijk bevestiging van de ontvangst van de melding.
- 3.4 De externe compliance officer registreert meldingen van incidenten op datum van ontvangst in het incidentenregister. Gedurende het verdere proces worden in het dossier relevante documenten opgenomen, zoals de communicatie tussen de verschillende betrokkenen, de rapportages en de resultaten van eventueel onderzoek.

4. Het onderzoek

- 4.1 Het Meldpunt bespreekt een binnengekomen melding met de directie. Het Meldpunt zal de directie adviseren de melding terzijde te leggen als uit een eerste analyse geen grond blijkt voor de melding.
- 4.2 Indien het Incident de bedrijfsvoering van een Opdrachtnemer betreft, wordt bij de afhandeling van het Incident zoveel mogelijk samengewerkt tussen Altera en de Opdrachtnemer.
- 4.3 Als de eerste analyse serieuze indicaties geeft van een mogelijk Incident, dan zal de directie de melding nader laten onderzoeken. De directie beoordeelt of er een separate onderzoekscommissie wordt ingesteld dan wel dat zij zelf het onderzoek leidt. Indien betrokkenheid van een van de directieleden wordt vermoed, zal direct de Raad van Commissarissen worden geïnformeerd, die vervolgens ook leiding aan het onderzoek zal geven. De externe compliance officer wordt gelijktijdig hierover geïnformeerd.
- 4.4 Wanneer de Melding een Datalek betreft, treedt de Procedure Datalekken in werking (zie bijlage). Alle andere Incidenten worden verder afgehandeld conform deze Incidentenregeling.
- 4.5 De Melder wordt geïnformeerd dat een onderzoek wordt ingesteld. De wijze van onderzoek en de termijn waarbinnen het onderzoek moet zijn afgerond, zijn afhankelijk van de aard van het Incident.

² Zie de Gedragscode van Altera voor de definitie van betrokkenen.

AlterA

- 4.6 De directie bewaakt de voortgang van het onderzoek.
- 4.7 Wanneer bij het onderzoek naar personen plaatsvindt, worden de bepalingen uit de privacywetgeving volledig in acht genomen.
- 4.8 De directie beslist welke eventuele gevolgen worden verbonden aan de uitkomsten van het onderzoek, na hierover de Raad van Commissarissen te hebben geïnformeerd.

5. Onderzoek naar een zwaar incident

- 5.1 In aanvulling op artikel 4, rapporteert de directie, wanneer de melding een zwaar Incident betreft, regelmatig over de voortgang van de afhandeling aan de Raad van Commissarissen en de externe compliance officer.
- 5.2 De algemeen directeur beslist over de communicatie, zowel intern als extern, met betrekking tot het zware Incident. De directie bepaalt of, in welke volgorde en op welk moment de volgende partijen op de hoogte dienen te worden gesteld en laat zich hierbij adviseren door de externe compliance officer en de Raad van Commissarissen:
 - a. de externe accountant;
 - b. de bewaarder;
 - c. de aandeelhouders;
 - d. de toezichthouder (AFM);
 - e. de pers;
 - f. het Openbaar Ministerie/de politie.

6. Uitkomst onderzoek

- 6.1 De onderzoeksresultaten worden door de directie gerapporteerd aan de Raad van Commissarissen en aan de externe compliance officer. De rapportage bevat een kort relaas van feiten en omstandigheden, de bewijsvoering in hoofdlijnen, de eventuele (tijd kritische) melding aan toezichthouder(s), alsmede het advies met betrekking tot de te nemen maatregel(en).

7. Maatregelen

- 7.1 Op basis van de onderzoeksresultaten beoordeelt de directie en besluit ten aanzien van eventuele aanpassing van procedures en overige maatregelen voor het herstel van de bedrijfsvoering.
- 7.2 Als het Incident zich bij een Opdrachtnemer heeft voorgedaan, is deze zelf verantwoordelijk voor de te treffen maatregelen. Altera wordt door de Opdrachtnemer over de te treffen maatregelen en de voortgang geconsulteerd en geïnformeerd.
- 7.3 Het veroorzaken van een Incident of anderszins daarbij betrokken zijn, kan leiden tot arbeidsrechtelijke maatregelen, waaronder ontslag op staande voet. In geval sprake is van opzettelijk en ernstige strafbare overtredingen, zoals misdrijven als genoemd in het Wetboek van Strafrecht en de Wet Economische Delicten, wordt in beginsel aangifte gedaan bij justitie of politie.
- 7.4 Namens het bestuur ziet de externe compliance officer toe op de implementatie en naleving van nieuwe procedures en maatregelen, die naar aanleiding van het Incident zijn getroffen.

8. Registratie

- 8.1 Het Meldpunt houdt door middel van een Incidentenregister een registratie bij van alle binnengekomen meldingen, de feiten en omstandigheden, de wijze van opvolging, ingestelde onderzoeken, onderzoeksresultaten, de genomen preventieve en repressieve maatregelen en de meldingen aan de toezichthouder(s). De systematische vastlegging is mede gericht op het inzichtelijk maken van Incidenten, zodat soortgelijke situaties voorkomen kunnen worden.

9. Rapportage

- 9.1 Het Meldpunt rapporteert over de Incidenten in de reguliere jaarrapportage op zodanige wijze dat de vertrouwelijkheid voldoende gewaarborgd blijft.

10. Externe melding

- 10.1 De directie kan naar aanleiding van het Incident aangifte doen bij de justitiële autoriteiten.
- 10.2 Daar waar van toepassing zal de directie, in overleg met de externe compliance officer, een melding doen bij de relevante toezichthouder(s). Indien het een Incident bij een Opdrachtnemer betreft, vindt tevens overleg met die partner plaats. Melding bestaat uit de relevante feiten en omstandigheden van het Incident, alsmede de maatregelen die naar aanleiding van het Incident zijn genomen of nog zullen worden genomen. De belangrijkste toezichthouders zijn De Autoriteit Financiële Markten en de Autoriteit Persoonsgegevens.

11. Bescherming

- 11.1 De Melder ondervindt geen negatieve gevolgen in welke zin dan ook, wanneer een melding te goeder trouw is gedaan.
- 11.2 Eenieder die uit hoofde van deze regeling informatie verkrijgt over (de melding van) een Incident betracht daarover uiterste geheimhouding tegenover derden, tenzij op basis van deze regeling of bij of krachtens de wet de bevoegdheid of de verplichting bestaat om die informatie aan een derde te verschaffen.

12. Slotbepaling

Deze Incidentenregeling kan door de directie gewijzigd worden. Deze Incidentenregeling treedt inwerking per 24 mei 2018.

Ondertekening

Amstelveen, 24 mei 2018

De directie van Altera Vastgoed NV

Bijlage

Procedure Datalekken

Per 25 mei 2018 is de Wet bescherming persoonsgegevens (Wbp) met de Wet meldplicht Datalekken vervangen door de Algemene Verordening Gegevensbescherming (AVG). De Wet meldplicht Datalekken is vanaf 25 mei 2018 verankerd in de AVG en dit betekent dat Altera een Datalek onverwijld moet melden aan:

- de Autoriteit Persoonsgegevens (AP) (artikel 33 AVG),
- in bepaalde gevallen aan de betrokkene(n) (artikel 34 AVG).

Deze procedure beschrijft hoe te handelen binnen Altera indien sprake is van:

- een Datalek of wanneer een Datalek binnen Altera vermoed wordt,
- een Datalek bij een Opdrachtnemer van Altera (bijvoorbeeld een vastgoedmanager en het salarisbureau, zijnde Verwerkers en/of overige Opdrachtnemers van Altera, zijnde makelaar, ontwikkelaar, aannemer).

Deze procedure is mede gebaseerd op de beleidsregels van Werkgroep 29 (Europese guidelines meldplicht datalekken). Zie hierbij de link

http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052

Per gemeld Datalek behoudt Altera zich de vrijheid voor om te beoordelen of de onderhavige procedure gevolgd moet worden, dan wel afwijking van deze procedure gerechtvaardigd is.

1. Definities

Naast de definities uit de Incidentenregeling zijn in de Procedure datalekken de volgende definities van kracht.

AP:

Autoriteit Persoonsgegevens.

AVG:

Algemene Verordening Gegevensbescherming (vanaf 25 mei 2018).

Betrokkene:

De natuurlijke persoon op wie een persoonsgegeven betrekking heeft (artikel 4 lid 1 AVG).

Beveiligingsincident³:

Een inbreuk op de beveiliging (zoals bedoeld in artikel 33 lid 1 AVG) waarbij het niet waarschijnlijk is dat de inbreuk in verband met persoonsgegevens een risico inhoudt voor de rechten en vrijheden van natuurlijke personen (bijvoorbeeld dat de persoonsgegevens niet zijn blootgesteld aan verlies of onrechtmatige verwerking); er is dan geen sprake van een Datalek.

Datalek⁴:

Een inbreuk op de beveiliging (zoals bedoeld in artikel 33 lid 1 en 34 AVG) waarbij het waarschijnlijk is dat de inbreuk in verband met persoonsgegevens een risico inhoudt voor de rechten en vrijheden van natuurlijke personen (bijvoorbeeld dat de persoonsgegevens zijn blootgesteld aan verlies of onrechtmatige verwerking); er is dan wel sprake van een Datalek.

Meldpunt:

Voor datalekken is het meldpunt de Functionaris Gegevensbescherming van de vennootschap en bij afwezigheid de Financieel directeur van Altera.

³ Laat de beoordeling of er sprake is van een beveiligingsincident/datalek (bijvoorbeeld door een verkeerd verzonden mail, gestolen telefoon, zoekgeraakt document) te allen tijde over het aan het Meldpunt. En meld het direct!

⁴ Laat de beoordeling of er sprake is van een beveiligingsincident/datalek (bijvoorbeeld door een verkeerd verzonden mail, gestolen telefoon, zoekgeraakt document) te allen tijde over het aan het Meldpunt. En meld het direct!

Persoonsgegevens:

Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon. Dit is nagenoeg alles van IP-adres, naam, adres en woonplaats, mailadres, telefoonnummer, kenteken, foto, maar ook identificatie nummer, locatiegegevens en alles wat maar iets zegt over een natuurlijk persoon (artikel 4 lid 1 AVG) .

Verwerker (artikel 4 lid 8 en 28 AVG):

De Opdrachtnemer die ten behoeve van Altera persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen. Het doel van en de middelen voor de gegevensverwerking wordt bepaald door de Verwerkingsverantwoordelijke. De Verwerker neemt geen beslissingen over het gebruik van de gegevens, de verstrekking aan derden en andere ontvangers, de duur van de opslag van de gegevens enz. Zou hij immers deze zeggenschap wel verwerven dan dient hij als Verwerkingsverantwoordelijke te worden aangemerkt (zoals bedoeld in artikel 4 lid 7 en artikel 24 AVG).

Verwerkingsverantwoordelijke (artikel 4 lid 7 en 24 AVG):

De partij die alleen of samen met anderen het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt (artikel 4 lid 7 AVG).

Verwerking van persoonsgegevens:

Elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens (artikel 4 lid 2 AVG).

Wbp:

Wet bescherming persoonsgegevens.

2. Identificeren Datalek

Een ieder die een Datalek vermoedt⁵ of constateert is verplicht zonder onnodige vertraging, doch uiterlijk binnen 48 uur na ontdekking, het Meldpunt bij Altera hiervan in kennis te stellen.

De Melder verschaft informatie over:

- a. de volledige feiten en omstandigheden van de constatering of het vermoeden;
- b. desgevraagd aanvullende gegevens die het Meldpunt nodig heeft om een eventueel onderzoek in te stellen en melding bij de toezichthouder te kunnen doen.

Met Opdrachtnemers die persoonsgegevens voor Altera verwerken (Verwerkers) zijn deze afspraken schriftelijk overeengekomen. Naast bovengenoemde informatie verschaft de Opdrachtnemer tevens informatie over de maatregelen die de Opdrachtnemer reeds heeft getroffen, of voorstelt te treffen, om de (negatieve) gevolgen van de inbreuk te beperken en te verhelpen.

3. Beoordeling Datalek ja/nee

Op basis van de verkregen informatie en bij het vermoeden van een Datalek wordt door de directie en de Functionaris Gegevensbescherming gezamenlijk zo spoedig mogelijk de beoordeling gemaakt of er daadwerkelijk sprake is van een Datalek. De externe compliance officer kan hierbij adviseren.

De beoordeling of sprake is van een Incident dat gemeld moet worden aan de AP, komt tot stand met behulp van de schema's te vinden in de beleidsregels van de Werkgroep 29 "Europese guidelines meldplicht datalekken"

http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052

Tevens wordt beoordeeld of per direct maatregelen genomen moeten worden om de schade te beperken, waaronder het doen van een (voorlopige) melding aan betrokkenen.

In geval dat het Incident niet heeft geleid tot verlies of onrechtmatige verwerking van persoonsgegevens, is geen sprake van een Datalek maar van een beveiligingsincident. Melding aan de AP is dan niet nodig. Wel overlegt de directie dan met de Functionaris Gegevensbescherming of het zinvol is om het beveiligingslek te onderzoeken om herhaling te voorkomen. De externe compliance officer wordt van de uitkomst en de overwegingen die tot het besluit hebben geleid op de hoogte gebracht.

4. Melden aan de Autoriteit Persoonsgegevens (Artikel 33 AVG)

De Functionaris Gegevensbescherming verzorgt, na afstemming met de directie, de tijdige (onverwijld, zonder onnodige vertraging en zo mogelijk niet later dan 72 uur na de ontdekking van het Datalek) elektronische melding bij de AP volgens het online meldingsformulier van de AP. De Functionaris Gegevensbescherming fungeert als contactpersoon inzake de communicatie naar de AP. Dit geldt ook in geval nog niet duidelijk is of het Incident een Datalek is.

Indien de concrete situatie zich daartoe leent, zal de directie aan de Opdrachtnemer vragen de melding aan de AP te doen en de directie en de Functionaris Gegevensbescherming op de hoogte te houden van de melding.⁶

5. Beoordeling of Datalek gemeld dient te worden aan betrokkene(n) (Artikel 34 AVG)

De directie stelt tezamen met de Functionaris Gegevensbescherming vast of het Datalek ook moeten worden gemeld aan degenen om wiens gegevens het gaat. Hierbij wordt ook gebruik gemaakt van de Europese guidelines meldplicht datalekken http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052

De externe compliance officer kan hierin adviseren.

6. Oorzaken en verbetermaatregelen bij de Opdrachtnemer

De Opdrachtnemer bij wie een Datalek is ontstaan is verplicht om bij constatering van een Datalek, in goed overleg met Altera, voor eigen rekening en risico alle noodzakelijke maatregelen te nemen om het Datalek te dichten en de schade die hieruit voortvloeit of kan vloeien te beperken. De Opdrachtnemer zal Altera volledig op de hoogte houden en blijven houden van de ontwikkelingen met betrekking tot het Datalek en de genomen of te nemen maatregelen, om de gevolgen hiervan te beperken en herhaling te voorkomen.

De directie zal aan de hand van de ontvangen informatie beoordelen of het noodzakelijk is aan de Opdrachtnemer te vragen bepaalde aanvullende beveiligingsmaatregelen te treffen. De directie bewaakt de voortgang ten aanzien van eventuele aanvullende beveiligingsmaatregelen.

⁵ Te allen tijde geldt hier dat een medewerker van Altera of Opdrachtnemer beter (achteraf) onnodig kan melden, dan besluiten een twijfelgeval niet te melden bij het Meldpunt. Beoordeling komt toe aan het Meldpunt.

⁶ Deze clausule geldt alleen voor Opdrachtnemers of andere derden, niet zijnde een Verwerker van Altera.

7. Registratie

Het Meldpunt van Altera registreert alle binnengekomen meldingen, de feiten en omstandigheden, de wijze van opvolging, ingestelde onderzoeken, onderzoeksresultaten, de genomen preventieve en repressieve maatregelen en de meldingen aan de toezichthouder. De systematische vastlegging is mede gericht op het inzichtelijk maken van Incidenten, zodat soortgelijke situaties voorkomen kunnen worden. Ieder Incident en Datalek wordt vastgelegd in het Verwerkingsregister (artikel 30 AVG).

De Opdrachtnemer houdt tevens een dergelijke registratie bij van ieder bij hem geconstateerd of vermoed Datalek.