Protocol van Cerium voor inbreuken in verband met persoonsgegevens in het kader van de Algemene Verordening gegevensbescherming (AVG)

betreffende procedures inzake de melding en afhandeling van inbreuken op de persoonsgegevens (datalekken)

We spreken van een inbreuk op de persoonsgegevens als persoonsgegevens in handen vallen van derden die geen toegang tot die gegevens zouden mogen hebben. Een inbreuk op de persoonsgegevens is het gevolg van een beveiligingsprobleem. In de meeste gevallen gaat het om uitgelekte computerbestanden, al kan een gestolen geprinte klantenlijst evengoed een inbreuk op de persoonsgegevens vormen. Andere voorbeelden: cyberaanvallen (incl. DDos), e-mail verzonden naar verkeerde adressen, gestolen laptops, afgedankte niet-schoongemaakte computers en verloren usb-sticks. Als een telefoon verloren of gestolen wordt, dan is dat mogelijk een inbreuk op de persoonsgegevens.

1. Inleiding

1.1. Dit document beschrijft de handelingen te verrichten door Cerium bij een inbreuk op de persoonsgegevens zoals gedefinieerd in de Algemene verordening gegevensbescherming (AVG).

1.2. Van een inbreuk op de persoonsgegevens is sprake als persoonsgegevens zijn blootgesteld aan verlies of onrechtmatige verwerking.

1.3. Een inbreuk op de persoonsgegevens dient onverwijld te worden gemeld aan de Autoriteit Persoonsgegevens (‘AP’), en in bepaalde gevallen ook aan de betrokkene(n). De betrokkene is degene van wie persoonsgegevens zijn gelekt.

1.4. De meldplicht is eveneens van toepassing op Cerium als die inbreuk op de persoonsgegevens bij een derde is ontstaan, bijvoorbeeld een verwerker van persoonsgegevens van Cerium (‘Verwerker’).

1.5. Waar in het navolgende sprake is van ‘gebruiker’ wordt daarmee bedoeld een ieder in welke hoedanigheid ook die gebruik maakt van of kennis neemt van bij Cerium aanwezige persoonsgegevens van natuurlijke personen en/of anderszins binnen Cerium organisatie actief is.

2. Identificatie van een inbreuk op de persoonsgegevens: organisatie

2.1. De gebruiker die een (mogelijk) inbreuk op de persoonsgegevens constateert, meldt dit incident per omgaande aan de door de directie van Cerium aangewezen functionaris gegevensbescherming (‘FG’) van Cerium.

2.2. Een gebruiker binnen Cerium of een Verwerker is te allen tijde bevoegd zelfstandig een melding te doen aan de FG. De procedure meldplicht inbreuken op de persoonsgegevens als omschreven in dit protocol wordt dan gestart.

3. Wanneer moet een inbreuk op de persoonsgegevens worden gemeld?

Niet alle incidenten hoeven aan de AP te worden gemeld. Alleen incidenten die voldoen aan de volgende criteria moeten worden gemeld:

- een incident dat een risico inhoudt voor de rechten en vrijheden van natuurlijke personen (bijvoorbeeld wegens mogelijke lichamelijke of (im)materiële schade, zoals discriminatie, identiteitsfraude, financieel verlies en reputatieschade (Art. 33 AVG);
- een incident met een hoog risico voor betrokkene(n) zal als regel ook aan de betrokkene(n) zelf gemeld moeten worden (Art. 34 AVG).

Of een inbreuk op de persoonsgegevens de AP en/of betrokkene(n) moet worden gemeld wordt onderstaand nader uitgewerkt.

4. Identificatie van een incident: is er sprake van een inbreuk op de persoonsgegevens?

4.1. De FG draagt zo spoedig mogelijk zorg voor het inventariseren en verzamelen van de informatie die benodigd is voor het (eventueel) melden van een inbreuk op de persoonsgegevens aan de AP. Daarbij kan het formulier van de AP voor het melden van inbreuken op de persoonsgegevens als uitgangspunt dienen. Het formulier is te vinden op het volgende adres: https://inbreuken op de persoonsgegevens.autoriteitpersoonsgegevens.nl/melding/aanmaken

4.2. Op basis van de verkregen informatie en bij het vermoeden van een inbreuk op de persoonsgegevens wordt in overleg tussen de directie, de FG en de eventuele overige verantwoordelijke en/of betrokken personen in de organisatie van Cerium of de betreffende Verwerker, beoordeeld of daadwerkelijk sprake is van een inbreuk op de persoonsgegevens.

4.3. In dat overleg kan tevens worden beoordeeld of er acuut maatregelen dienen te worden genomen om de schade zoveel mogelijk te beperken, waaronder het doen van een (voorlopige) melding aan betrokkene(n). Indien nodig kan advies gevraagd worden aan de juridisch adviseur en/of de communicatieadviseur, indien aanwezig.

4.4. Wanneer er sprake is van een incident dat gemeld moet worden aan de AP kan gebruik worden gemaakt van de overzichten in de beleidsregels ‘Meldplicht inbreuken op de persoonsgegevens in de Wet bescherming persoonsgegevens’ van de AP, te vinden op het volgende adres: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/richtsnoeren_meldplicht_datalekken_0.pdf

4.5. Bij de beoordeling van de vraag of sprake is van een inbreuk op de persoonsgegevens zijn de volgende factoren van belang:

- is er sprake van onrechtmatige verwerking van persoonsgegevens?

hiermee wordt onder andere gedoeld op de onbedoelde of onwettige vernietiging, verlies of wijziging van verwerkte persoonsgegevens of een niet toegestane toegang tot verwerkte persoonsgegevens of de niet toegestane verstrekking daarvan;

- Is er sprake van verlies van persoonsgegevens?

  dit betekent dat Cerium (of feitelijk haar Verwerker) deze gegevens niet meer heeft, omdat ze zijn vernietigd of op een andere wijze verloren zijn gegaan;

- is er sprake van een enkele tekortkoming of kwetsbaarheid in de beveiliging?
- kan er redelijkerwijs worden uitgesloten dat een inbreuk op de beveiliging tot een onrechtmatige verwerking heeft geleid?
- zijn er persoonsgegevens van gevoelige aard gelekt?

- leiden de aard en de omvang van de inbreuk tot (een aanzienlijke kans op) ernstige nadelige gevolgen?

4.6. Indien het incident niet heeft geleid tot verlies of onrechtmatige verwerking van persoonsgegevens is er geen sprake van een inbreuk op de persoonsgegevens maar van een beveiligingslek. In dat geval is melding aan de AP niet nodig.

4.7. Indien tot de conclusie wordt gekomen dat sprake is van een (mogelijk) inbreuk op de persoonsgegevens, wordt het communicatietraject richting betrokkene(n) en (eventueel) de betreffende Verwerker tussen de directie van Cerium en de FG besproken.

5. Melden aan de Autoriteit Persoonsgegevens

5.1. De directie van Cerium of de FG verzorgt de tijdige melding bij de AP volgens het hierboven onder 4.1 genoemde meldingsformulier van de AP. De melding dient op grond van de AVG onverwijld, zonder onnodige vertraging en zo mogelijk niet later dan 72 uur na de ontdekking van het inbreuk op de persoonsgegevens te geschieden. De directie wordt tevens op de hoogte gesteld van de melding.
Als aan de termijn van 72 uur niet kan worden voldaan, dient de melding vergezeld te gaan van een reden voor het niet aanhouden van de termijn

5.2. De FG, of, bij ontstentenis daarvan, de directie van Cerium, fungeert als contactpersoon inzake de communicatie met de AP. Afhankelijk van de aard van de inbreuk op de persoonsgegevens of indien blijkt dat het incident geen inbreuk op de persoonsgegevens is kan de melding aan de AP worden aangevuld of ingetrokken.

5.3. De directie of, op verzoek van de directie, de FG draagt ervoor zorg dat de bij het incident betrokken gebruikers worden geïnformeerd en vraagt de bij het incident betrokken gebruikers zo snel mogelijk een verslag op te stellen over de toedracht van het incident. Deze schriftelijke informatie wordt aan de directie en de FG verstrekt ten behoeve van het ‘inbreuken op de persoonsgegevens’-dossier van Cerium.

5.4. Na ontvangst van de melding aan de AP zal de AP daarvan een ontvangstbevestiging sturen. De AP neemt alleen contact op indien de AP daartoe aanleiding ziet.

6. Is sprake van een hack?

Bij een inbreuk op de persoonsgegevens als gevolg van een (niet-ethische) hack (artikel 138ab Wetboek van Strafrecht), is het van belang om vast te stellen wat de aard van de gelekte persoonsgegevens is en wat de risico’s van misbruik voor de betrokkene(n) zijn. Bij een hack kan het naast het doen van de melding bij de AP ook zinvol zijn om aangifte te doen bij de politie. De FG zal daarvoor in dat geval in overleg met de directie van Cerium zorgdragen.

7. Dient de inbreuk op de persoonsgegevens te worden gemeld aan betrokkene(n)?

7.1. Indien een inbreuk op de persoonsgegevens is gemeld aan de AP dient te worden vastgesteld of de inbreuk op de persoonsgegevens ook moeten worden gemeld aan degenen om wiens persoonsgegevens het gaat. De directie zal dat in overleg met de FG vaststellen.

7.2. De beoordeling of er sprake is van een incident dat gemeld moet worden aan de betrokkenen kan tot stand komen met behulp van de overzichten in de beleidsregels 'Meldplicht inbreuken op de persoonsgegevens in de Wet bescherming persoonsgegevens' van de AP zoals hierboven genoemd.

7.3. Bij de afweging of het inbreuk op de persoonsgegevens dient te worden gemeld aan betrokkene(n) is onder andere het volgende van belang:

- indien Cerium passende technische beschermingsmaatregelen heeft genomen waardoor de persoonsgegevens die het betreft onbegrijpelijk of ontoegankelijk zijn voor een ieder die geen recht heeft op kennisname van de gegevens, dan kan de melding aan de betrokkene(n) achterwege blijven. Indien daarover wordt getwijfeld dan dient het inbreuk op de persoonsgegevens aan de betrokkene(n) gemeld te worden;

- de inbreuk op de persoonsgegevens moet aan de betrokkene(n) worden gemeld indien de inbreuk waarschijnlijk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer;

Betrokkenen kunnen door het verlies, onrechtmatig gebruik of misbruik van persoonsgegevens in hun belangen worden geschaad. De schade kan van materiële of van immateriële aard zijn, waarbij kan worden gedacht aan onrechtmatige publicatie, aantasting in eer en goede naam, identiteitsfraude of discriminatie;

7.4. De melding aan de betrokkene(n) mag achterwege blijven als daarvoor zwaarwegende redenen aanwezig zijn. De melding mag alleen achterwege mag blijven als dit *noodzakelijk* is met het oog op de belangen die worden genoemd in de AVG

8. Handelwijze melding aan betrokkene(n)

8.1. In opdracht van de directie van Cerium stelt de FG een kennisgeving aan betrokkene(n) op. De FG bepaalt wat aan de betrokkene(n) wordt gemeld.

8.2. De melding bevat in ieder geval de aard van de inbreuk, contactgegevens van Cerium en een contactpersoon of informatiepunt waar de betrokkene(n) meer informatie over de inbreuk kan (kunnen) krijgen, en de maatregelen die Cerium de betrokkene(n) aanbeveelt om te nemen om de negatieve gevolgen van de inbreuk te beperken.

8.3. De inbreuk op de persoonsgegevens moet onverwijld gemeld worden aan de betrokkene(n). Dit betekent dat Cerium na het ontdekken van de inbreuk op de persoonsgegevens enige tijd mag nemen voor nader onderzoek zodat Cerium de betrokkene op een behoorlijke en zorgvuldige manier kan informeren. Daarbij dient te allen tijde rekening te worden gehouden met het (eventuele) feit dat de betrokkene(n) naar aanleiding van de melding mogelijk maatregelen moet(en) nemen om zich te beschermen tegen de gevolgen van het inbreuk op de persoonsgegevens. Hoe eerder de betrokkene(n) daarover wordt geïnformeerd, hoe eerder deze in actie kan komen.

8.4. De betrokkene(n) worden *individueel* geïnformeerd.

8.5. In de melding aan de AP is aangegeven of de inbreuk op de persoonsgegevens aan betrokkene(n) is gemeld. Indien de aan de AP aangegeven termijn waarbinnen die melding zou worden gedaan aan de betrokkene(n) niet kan worden gehaald dan dient de FG dit aan de AP door te geven door middel van een aanpassing van de eerdere melding.

9. Inbreuk op de persoonsgegevens: onderzoek en vaststellen verbetermaatregelen

9.1. De FG stelt zo spoedig mogelijk na de vaststelling van het incident een (intern) onderzoek in naar de feitelijke toedracht van de (mogelijke) inbreuk op de persoonsgegevens en betrekt daarbij de vraag of en hoe dergelijke incidenten in de toekomst kunnen worden voorkomen.

9.2. In overleg met de directie van Cerium mag de FG daartoe met gebruikers binnen Cerium en/of overige relevante personen (zoals eventueel medewerkers van de Verwerker(s) van Cerium) spreken, alle relevante documenten inzien en toegang hebben tot alle plaatsen, voor zover noodzakelijk voor een zorgvuldig onderzoek;

9.3. De FG kan de directie van Cerium voorstellen om waar nodig externe partijen te betrekken indien dat voor een deugdelijk onderzoek noodzakelijk is.

9.4. De FG rapporteert de conclusies van het hiervoor bedoelde onderzoek zo spoedig mogelijk aan de directie van Cerium.

9.5. In overleg waarbij in ieder geval de directie van Cerium en de FG aanwezig zijn zullen de uitkomsten van het hiervoor genoemde onderzoek worden besproken en afspraken worden gemaakt over verbetermaatregelen om herhaling van het incident zoveel mogelijk te voorkomen.

9.6. De directie van Cerium ziet er op toe dat de vastgestelde verbetermaatregelen worden geïmplementeerd en in de organisatie van Cerium (en waar nodig extern, zoals aan een Verwerker) worden gecommuniceerd.

10. Inbreuk op de persoonsgegevens: dossier (datalek register)

Het ‘inbreuk op de persoonsgegevens’-dossier wordt digitaal bij de FG bewaard voor de duur van minimaal 1 jaar.

Aldus op 30 april 2018 vastgesteld door de directie van Cerium