Draaiboek meldplicht datalekken

1. Inleiding

1.1. Sinds 1 januari 2016 is er een Meldplicht Datalekken van kracht geworden. Deze meldplicht houdt in dat organisaties onverwijld een melding moeten doen bij de Autoriteit Persoonsgegevens (‘AP’) zodra sprake is van een ernstig datalek. In een aantal gevallen moet dit ook aan de betrokkenen (degenen van wie de persoonsgegevens zijn gelekt) gemeld worden.

1.2. Om het bovenstaande zoveel mogelijk in goede banen te leiden is dit draaiboek opgesteld. Hierin is praktisch vastgelegd hoe het Centrum Voor Dienstverlening (CVD) dient te handelen wanneer (mogelijk) sprake is van een datalek. Het doel hiervan is om zorgvuldige omgang met een (mogelijk) datalek te borgen en daarmee (ook) de schade en aansprakelijkheid van CVD zoveel mogelijk te beperken.

1.3. Met de komst van de Algemene Verordening Gegevensbescherming zijn de eisen die worden gesteld aan het melden van datalekken vastgelegd. In dit draaiboek zijn deze eisen verwerkt waarmee het draaiboek ‘AVG proof’ is geworden.

2. Reikwijdte en implementatie

2.1. Het beleid zoals opgenomen in dit draaiboek geldt vanaf 25-05-2018 en is per 2 april 2021 gereviseerd.

2.2. Alle leidinggevenden dragen er zorg voor dat de werknemers waarvoor zij verantwoordelijk zijn op de hoogte zijn van het bestaan van dit Draaiboek en de procedure die hierin opgenomen is. Als werknemers hierover vragen hebben kunnen zij terecht bij hun leidinggevende.

2.3. Het draaiboek wordt elke 2 jaar gereviseerd of zoveel vaker als in verband met gewijzigde regelgeving noodzakelijk is. Ook vindt revisie plaats in geval van een substantieel datalek. De meest recente versie is toegankelijk via het digitale Kwaliteitshandboek (onderdeel van AFAS).

3. Definities

3.1. Betrokkene: degene op wie een persoonsgegeven betrekking heeft.

3.2. Datalek: een inbreuk op de beveiliging die leidt tot de aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van Persoonsgegevens.

3.3. Persoonsgegeven: elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon.

3.4. Verwerking: elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens.

Daaronder wordt in ieder geval verstaan het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van ter beschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwisselen of vernietigen van gegevens. Onder deze term vallen cliënt- en klantdossiers en dossiers van medewerkers van CVD.

3.5. Verwerkingsverantwoordelijke: de directeur-bestuurder van CVD of diens waarnemer.

4. Procedure

Onverwijlde mededeling

4.1. Eenieder die een (mogelijk) datalek constateert meldt dit onverwijld aan zijn/haar leidinggevende. Indien de constatering buiten werktijd plaatsvindt, wordt zo spoedig mogelijk doch uiterlijk binnen 24 uur via de Afas startpagina middels het icoon Melding Datalek contact opgenomen met de Functionaris Gegevensbescherming (FG) en Coördinator Informatiebeveiliging (CIV).

4.2. Indien de leidinggevende of de melder van oordeel is dat mogelijk sprake is van een datalek meldt hij/zij dit onverwijld aan de Functionaris Gegevensbescherming (FG). Wanneer de leidinggevende de melder twijfelen of sprake is van een datalek wordt dit eveneens gemeld bij de FG en de CIV of diens waarnemer.

4.3. Alle coördinatie en communicatie aangaande het (vermeende) datalek verloopt uitsluitend via de FG of diens waarnemer. Een ieder is gehouden alle verzoeken van externen, waaronder de media, door te verwijzen naar de FG of diens waarnemer.

4.4. De FG beoordeelt vervolgens onverwijld of (i) mogelijk sprake is van een Datalek en (ii) of CVD voor het melden van dit Datalek de verantwoordelijkheid draagt.

4.5. Indien de FG of diens waarnemer (CIV) door omstandigheden afwezig, dan wel onbereikbaar is, fungeert de directeur/bestuurder of diens waarnemer als zijn waarnemer.

Onderzoek

4.6. Indien de FG van oordeel is dat sprake is van een datalek waarvoor CVD de verantwoordelijkheid draagt dan wordt onderzocht hoe dit lek is ontstaan en welke (preventieve) beschermingsmaatregelen ingezet worden.

4.7. Als besloten wordt om de oorzaak van het datalek niet te onderzoeken dient de reden hiervoor gedocumenteerd te worden. Indien de reden is dat CVD hiervoor niet de (formele) verantwoordelijkheid draagt dan informeert de FG onverwijld de organisatie die wél de verantwoordelijkheid draagt voor het melden van het datalek.

4.8. De FG heeft de leiding over het onderzoek en kan hierbij zowel de hulp van anderen binnen de organisatie als (in overleg met de directie) buiten de organisatie inschakelen (‘Datalek Onderzoeksteam’). De FG rapporteert over de voortgang en (voorlopige) uitkomst van het onderzoek aan de directie.

4.9. Het Datalek Onderzoeksteam onderzoekt vervolgens het desbetreffende datalek en stelt vast hoe de negatieve gevolgen van het lek zoveel mogelijk beperkt kunnen worden. Daarbij neemt het Datalek Onderzoeksteam in ieder geval de volgende zaken in overweging:

- de datum waarop het datalek is ontstaan;
- hoe het datalek is ontstaan;
- hoe het datalek is ontdekt;
- de aard en ernst van het datalek;
- de omvang van het datalek;
- of het datalek specifieke (kwetsbare) groepen personen betreft;
- of de verloren, gestolen of geschonden Persoonsgegevens zijn hersteld;
- of er aangifte bij de politie is gedaan/gedaan moet worden;
- of het datalek, althans enige schade die hieruit is voortgevloeid, bij de verzekering gemeld moet worden;
- of eventueel een advocaat in de arm genomen moet worden[1];
- welke (preventieve) beschermingsmaatregelen genomen zijn/kunnen worden om de gevolgen van het datalek zoveel mogelijk te beperken en welke kosten dit met zich meebrengt;
- wat er met de Persoonsgegevens gebeurt (is) en welke gevolgen dit heeft gehad/zou kunnen hebben;
- overige consequenties (zoals een risico voor de algemene gezondheid of het verlies van reputatie).

4.10. Bovenstaande bevindingen worden schriftelijk vastgelegd en door de FG in concept voorgelegd aan de directie. De directie kan vervolgens opdracht geven nader of diepgaander onderzoek te verrichten.

4.11. Dit onderzoek geniet een hoge prioriteit en dient -indien mogelijk- binnen 2 werkdagen afgerond te zijn nadat het gerapporteerd is door de leidinggevende aan de FG en CIV.

4.12. Nadat de belangrijkste kwesties zijn onderzocht en er zo spoedig mogelijk eventueel (preventieve) beschermingsmaatregelen zijn getroffen wordt indien noodzakelijk en op verzoek van de directie, door (een deel van) het Datalek Onderzoeksteam diepgaander onderzoek verricht naar (de oorzaak en de gevolgen van) het datalek.

(Preventieve) beschermingsmaatregelen

4.13. Indien het Datalek Onderzoeksteam heeft vastgesteld dat er preventieve beschermingsmaatregelen genomen moeten worden om de (mogelijke) gevolgen van het (mogelijke) datalek in een vroegtijdig stadium te beperken, komen -afhankelijk van de aard en omvang van het lek- de volgende maatregelen in aanmerking:

- het veranderen van toegangscodes en wachtwoorden voor apparaten en/of systemen en/of het blokkeren van (een) account(s);
- het zoeken/opsporen van het verloren/gestolen (deel van een) goed/apparaat;
- het isoleren of afsluiten van een (deel van) het netwerk/systeem;
- het gebruik maken van back-ups om verloren/gestolen gegevens te herstellen;

[1] Een advocaat kan adviseren of een melding aan de AP en Betrokkenen noodzakelijk is. Informatie-uitwisseling met een advocaat is vertrouwelijk en kan nadien in beginsel niet worden opgevraagd door de AP.

- het identificeren van de (mogelijke) betrokkenen die op de hoogte gesteld moeten worden van het (mogelijke) datalek en hen, indien nodig, alvast instructies geven en/of assisteren ter voorkoming van eventuele schade van het datalek;
- het informeren van betrokken organisaties die advies kunnen geven en/of moeten krijgen om het datalek zo snel mogelijk te verhelpen en de (mogelijke) gevolgen hiervan zoveel mogelijk te beperken. [2]
- Het informeren van de directie opdat deze zich vast voor kan bereiden op de berichtgeving naar buiten en/of aan (eventuele) betrokkenen en/of vragen van de pers;
- het doen van aangifte bij de politie in gevallen waarin (waarschijnlijk) sprake is (geweest) van illegale activiteiten of wanneer dit in de toekomst verwacht kan worden (denk hierbij aan identiteitsfraude, hacking etc.);
- enige andere maatregel die in het specifieke geval noodzakelijk wordt geacht.

4.14. Het treffen van (voorlopige) beschermingsmaatregelen gebeurt altijd in overleg en met goedkeuring van de directie.

Melding aan de AP

4.15. De FG beoordeelt (zo mogelijk op basis van het afgeronde onderzoek) in overleg met de directie of een melding aan de AP noodzakelijk is. In dat geval dient de melding plaats te vinden binnen 72 uur nadat de verwerkingsverantwoordelijke zich bewust is geworden van een datalek.

4.16. De meldplicht is niet van toepassing als het onwaarschijnlijk is dat de inbreuk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen.

4.17. Elk datalek, ook indien dit niet leidt tot een melding, dient door de FG te worden opgenomen in het eigen CVD-datalekkenregister. Geregistreerd dienen in elk geval te worden de feiten omtrent het datalek, de gevolgen en de genomen corrigerende maatregelen (zodat de AP in staat is naleving van de AVG te controleren).

4.18. De melding van een datalek moet worden ingediend door het daartoe door de AP beschikbaar gestelde webformulier ‘Meldloket Datalekken’[3] in te vullen.

4.19. Indien de melding later dan na 72 uur (zie artikel 4.16) geschiedt dient door de verwerkingsverantwoordelijke een verklaring te worden gegeven waarom de melding niet eerder gedaan is. De melding kan later altijd nog worden aangevuld of ingetrokken.

Melding aan betrokkene

4.20. Nadat een melding aan de AP is gedaan onderzoekt de FG -eventueel gesteund door (een deel van) het Datalek Onderzoeksteam- in samenspraak met de directie of het datalek gemeld dient te worden aan de betrokkene.[4] Dit is het geval wanneer het waarschijnlijk is

[2] Als er bijvoorbeeld bankgegevens verloren/gestolen zijn kunnen eventueel de desbetreffende banken benaderd worden om te adviseren hoe fraude zoveel mogelijk voorkomen kan worden.

[3] Zie: https://Datalekken.autoriteitpersoonsgegevens.nl/actionpage?0

[4] Indien het datalek volgens de wet niet aan de AP gemeld hoeft te worden hoeft dit ook niet aan de betrokkenen(n) te worden gemeld.

dat de inbreuk resulteert in een hoog risico voor de rechten en vrijheden van de betrokkene zodat hij/zij eventueel voorzorgsmaatregelen kan treffen.

4.21. Indien de directie besluit dat een melding aan de betrokkene(n) noodzakelijk is, bepaalt ze tevens hoe deze kennisgeving dient plaats te vinden. Hierbij kan er afhankelijk van de omstandigheden aan gedacht worden om alle betrokken individueel dan wel gezamenlijk te informeren dan wel te kiezen voor een combinatie daarvan.

4.22. Daarnaast beslist de directie welke communicatiemiddelen voor de kennisgeving ingezet worden (e-mail, post, berichtgeving op de eigen website, kranten etc.) en wordt een tekst voor de kennisgeving [5]vastgesteld welke in elk geval de volgende elementen omvat:
- de aard van de inbreuk;
- de instanties waar meer informatie over de inbreuk kan worden verkregen;
- de aanbevolen maatregelen om de negatieve gevolgen van de inbreuk te beperken.

4.23. Een melding aan de betrokkene kan achterwege blijven wanneer er maatregelen zijn getroffen conform de Algemene Verordening Gegevensbescherming en deze zijn toegepast op de betreffende persoonsgegevens (zoals pseudonimisering). Een melding kan ook achterwege blijven als achteraf maatregelen zijn genomen door de verwerkingsverantwoordelijke om te zorgen dat de hoge risico's voor de rechten en vrijheden van de betrokkene zich waarschijnlijk niet meer zullen voordoen.

4.24. Indien de mededeling aan de betrokkene onevenredige inspanning van de verwerkingsverantwoordelijke vergt, kan de mededeling achterwege blijven en moet(en) de betrokkene(n) op een andere, even doeltreffende manier worden geïnformeerd (bijvoorbeeld door een openbare mededeling).

Beoordeling en evaluatie

4.25. Zodra alle initiële zorgen omtrent het datalek verholpen zijn actualiseert de FG het overzicht met alle datalekken. Dit overzicht bevat in ieder geval feiten en gegevens omtrent de aard van de inbreuk, de melding aan de AP en, indien een melding aan de betrokkene(n) is gedaan, de tekst van de kennisgeving aan de betrokkene(n).

4.26. De gegevens worden -behoudens het gestelde in artikel 4.28- gedurende een jaar na het ontstaan van het datalek bewaard (om lering te trekken uit het datalek en antwoord te kunnen geven op vragen van betrokkene(n) of het datalek, indien nodig, later alsnog aan betrokkene(n) te melden). Dit overzicht wordt niet openbaar gemaakt.

4.27. In afwijking van artikel 4.27 geldt een bewaartermijn van drie jaar wanneer geen melding van het datalek aan de betrokkene(n) is gedaan omdat a) geoordeeld is dat de technische beschermingsmaatregelen voldoende bescherming boden of b) er sprake was van zwaarwegende omstandigheden. De FG evalueert -in overleg met de directie- eenmaal per jaar of het datalek alsnog aan de betrokkene(n) gemeld moet worden.

4.28. De directie neemt aan de hand van de evaluatie in overweging of:
- nog diepgaander onderzoek gedaan moet worden naar (het ontstaan en/of de gevolgen van) het datalek;

[5] Volgens de wet dient de kennisgeving aan de Betrokkene op zo'n manier gedaan te worden dat, rekening houdend met de aard van de inbreuk, de geconstateerde en feitelijke gevolgen daarvan voor de verwerking van persoonsgegevens, de kring van de Betrokkenen en kosten van tenuitvoerlegging, een behoorlijke en zorgvuldige informatievoorziening is gewaarborgd.

- een actieplan/prioriteitenlijst opgesteld moet worden om toekomstige/verwachte problemen systematisch aan te pakken.