PCBO Leeuwarden e.o.

Procedure beveiligingsincident en weging meldplicht datalek

Afwegingen in het kader van artikel 13 Wet Bescherming Persoonsgegevens

VERENIGING VOOR PROTESTANTS CHRISTELIJK BASISONDERWIJS LEEUWARDEN EN OMSTREKEN
MARG. DE HEERSTRAAT 2, 8921 AK LEEUWARDEN
POSTBUS 1090, 8900 CB LEEUWARDEN
TEL.: 058-2130350
E-mail : info@pcboleeuwarden.nl

Procedure beveiligingsincident en weging meldplicht datalek

Karakter: De inhoud van deze procedure wordt geacht bekend te zijn bij alle medewerkers van PCBO Leeuwarden e.o. en worden nageleefd in het geval van een datalek

Doel: Deze procedure maakt deel uit van het privacyreglement van PCBO Leeuwarden e.o. De hieronder uiteengezette procedure voorziet in een stappenplan ten aanzien van een beveiligingsincident en de afwegingen over de meldplicht datalekken (artikel 13 Wet Bescherming Persoonsgegevens (Wbp))

---

0. Beveiligingskwetsbaarheid

Vraag
Is er sprake van een kwetsbaarheid in een systeem of een werkwijze waarbij persoonsgegevens verwerkt worden?

Toelichting
De medewerkers van PCBO Leeuwarden e.o. of afnemers zijn verplicht zwakke plekken in de beveiliging of werkwijze (of het vermoeden daarvan) te melden. Een dergelijke verplichting is erop gericht tekortkomingen zo snel mogelijk te ontdekken en te kunnen oplossen.
De medewerkers van PCBO Leeuwarden e.o. of afnemer zijn eveneens verplicht onvolkomenheden in de programmatuur (of vermoeden daarvan) op het terrein van beveiliging te melden. Een dergelijke verplichting is erop gericht onvolkomenheden in de programmatuur zo snel mogelijk te ontdekken en te kunnen oplossen.

Bespreken
Met functionaris bescherming personeelsgegevens, mevr. mr. E. van der Molen.

1. Beveiligingsincident

Vraag
Zijn bij het beveiligingsincident persoonsgegevens verloren gegaan, of is onrechtmatige verwerking redelijkerwijs niet uit te sluiten?

Toelichting
Er is alleen sprake van een datalek als zich daadwerkelijk een beveiligingsincident heeft voorgedaan. Bij een beveiligingsincident denken we bijvoorbeeld aan het kwijtraken van een USB-stick, foutief verstuurde bestanden, de diefstal van een laptop of aan een inbraak door een hacker.
Maar niet ieder beveiligingsincident is ook een datalek. Er is sprake van een datalek als er bij het beveiligingsincident persoonsgegevens verloren zijn gegaan, of als onrechtmatige verwerking van de persoonsgegevens niet redelijkerwijs kan worden uitgesloten.

Definitie
Een incident is ieder voorval of gebeurtenis die schade toebrengt of kan toebrengen aan de beveiliging van het systeem. Hiermee wordt bedoeld iedere inbreuk op het gebied van beschikbaarheid, integriteit (betrouwbaarheid) en/of vertrouwelijkheid (exclusiviteit).
Een handeling die in strijd is met de beveiligingsprocedures van PCBO Leeuwarden e.o. is ook een beveiligingsincident.

Verantwoordelijkheid
Iedere gebruiker van het systeem, die direct of indirect kennis draagt of krijgt van een incident of bijna incident als hier omschreven, is verplicht dit te melden aan de leidinggevende.

Indien het (bijna) incident wordt gemeld aan de leidinggevende, zorgt deze er voor dat het incident gemeld wordt bij functionaris bescherming personeelsgegevens, mevr. mr. E. van der Molen.

Uitvoering
1.
Elke medewerker van PCBO is verplicht een beveiligingsincident te melden aan de leidinggevende. Deze meldt het beveiligingsincident bij functionaris bescherming personeelsgegevens, mevr. mr. E. van der Molen. Welke deze registreert als beveiligingsincident.

2.
Functionaris bescherming personeelsgegevens, mevr. mr. E. van der Molen onderzoekt het (bijna) incident. Bij dit onderzoek wordt aandacht besteed aan de volgende aspecten:

- wat is de aard van het (bijna) incident;
- wat is de oorzaak dat dit (bijna) incident heeft plaatsgevonden;
- is er sprake van het niet nakomen van of een tekortkoming in de beveiligingsprocedures;
- is het (bijna) incident verwijtbaar;
- is een eventuele tekortkoming in de beveiliging inmiddels hersteld;
- kan dit (bijna) incident nogmaals optreden
- welke acties moeten worden getroffen om herhaling te voorkomen
- of er wellicht sprake is van een datalek in de zin van de Wet Bescherming Persoonsgegevens en de daaraan gekoppelde Meldplicht Datalekken. Als dit wordt vermoed, wordt het incident verder besproken in het spoedoverleg zoals hieronder weergegeven.

3.
Functionaris bescherming personeelsgegevens, mevr. mr. E. van der Molen stelt van het onderzoek een kort verslag op. De essentie van het verslag wordt opgenomen in de jaarlijkse managementrapportage. Bij een groot incident wordt het verantwoordelijk bestuur op de hoogte gebracht van de aard en afhandeling.

Als dit het geval is en er is sprake van een daadwerkelijk lek van onversleutelde gegevens, zoals benoemd in de Meldplicht Datalekken, dan zal dit binnen 72 uur na vinden van het lek gemeld moeten worden bij het de Autoriteit Persoonsgegevens.

4.
Ingeval van overtreding van de beveiligingsvoorschriften kunnen er door PCBO Leeuwarden e.o. disciplinaire maatregelen getroffen worden.
Onder “disciplinaire maatregelen” worden verstaan: de disciplinaire maatregelen als bedoeld in de CAO PO.

2. Datalek

Vraag
Gaat het om persoonsgegevens van gevoelige aard, of is er om een andere reden sprake van (een aanzienlijke kans op) ernstige nadelige gevolgen voor de bescherming van de verwerkte persoonsgegevens?

Toelichting
Niet ieder datalek hoeft te worden gemeld aan de Autoriteit Persoonsgegevens. Volgens de wet moet er een melding gedaan worden aan de Autoriteit Persoonsgegevens als het datalek leidt tot een aanzienlijke kans op

ernstige nadelige gevolgen voor de bescherming van persoonsgegevens, of als het ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens.
Een factor die hierbij een rol speelt is de aard van de gelekte persoonsgegevens. Als er persoonsgegevens van gevoelige aard zijn gelekt, dan is over het algemeen een melding noodzakelijk. Bij persoonsgegevens van gevoelige aard moeten we denken aan:
• *Bijzondere persoonsgegevens zoals bedoeld in artikel 16 Wbp* Het gaat hierbij om persoonsgegevens over iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, lidmaatschap van een vakvereniging en om strafrechtelijke persoonsgegevens en persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag.
• *Gegevens over de financiële of economische situatie van de betrokkene* Hieronder vallen bijvoorbeeld gegevens over (problematische) schulden, salaris- en betalingsgegevens.
• *(Andere) gegevens die kunnen leiden tot stigmatisering of uitsluiting van de betrokkene* Hieronder vallen bijvoorbeeld gegevens over gokverslaving, prestaties op school of werk of relatieproblemen.
• *Gebruikersnamen, wachtwoorden en andere inloggegevens* De mogelijke gevolgen voor betrokkenen hangen af van de verwerkingen en van de persoonsgegevens waar de inloggegevens toegang toe geven. Bij de afweging moet worden betrokken dat veel mensen wachtwoorden hergebruiken voor verschillende verwerkingen.
• *Gegevens die kunnen worden misbruikt voor (identiteits)fraude* Het gaat hierbij onder meer om biometrische gegevens, kopieën van identiteitsbewijzen en om het Burgerservicenummer (bsn).
Ook andere factoren, zoals de hoeveelheid gelekte persoonsgegevens per persoon of het aantal betrokkenen van wie er persoonsgegevens zijn gelekt, kunnen aanleiding zijn om het datalek te melden. Maar let op: als de aard van de gelekte gegevens daar aanleiding toe geeft is het mogelijk dat er een datalek moet worden gemeld waar de persoonsgegevens van slechts één persoon bij betrokken zijn.
De melding moet worden gedaan zonder onnodige vertraging en zo mogelijk niet later dan 72 uur na de ontdekking van het datalek. Op de website van de Autoriteit Persoonsgegevens is voor dit doel een webformulier beschikbaar. Via dit webformulier kan de melding zo nodig worden aangevuld of ingetrokken.

3. Melden aan de Autoriteit Persoonsgegevens

Vraag:
Waren niet alle gelekte gegevens (goed) versleuteld, of heeft het datalek om andere redenen waarschijnlijk ongunstige gevolgen voor de persoonlijke levenssfeer van de betrokkene?

Toelichting:
Als er tot de conclusie gekomen wordt dat een datalek moet worden gemeld aan de Autoriteit Persoonsgegevens, dan betekent dit niet automatisch dat dit datalek ook moet worden gemeld aan de betrokkene. Hiervoor moet een aparte afweging worden gemaakt.
De wet geeft aan dat een melding moet worden gedaan aan de betrokkene als het datalek waarschijnlijk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer. Betrokkenen kunnen door het verlies, onrechtmatig gebruik of misbruik in hun belangen worden geschaad. Daarbij moeten we bijvoorbeeld denken aan onrechtmatige publicatie, aantasting in eer en goede naam, (identiteits)fraude of discriminatie. Als er persoonsgegevens van gevoelige aard zijn gelekt, dan kunnen we er in principe van uit gaan dat het datalek niet alleen moet worden gemeld aan de Autoriteit Persoonsgegevens, maar ook aan de betrokkene.

4. Melden aan de betrokkene

Vraag:
Zal het datalek waarschijnlijk ongunstige gevolgen hebben voor de persoonlijke levenssfeer van betrokkene?

Toelichting:

Betrokkenen kunnen door verlies, onrechtmatig gebruik of misbruik van persoonsgegevens in hun belangen worden geschaad. De schade kan van materiele of immateriële aard zijn. Bij dit laatste moeten we denken aan onrechtmatige publicatie, aantasting in eer en goede naam, identiteitsfraude of discriminatie. Identiteitsfraude kan overigens niet alleen leiden tot immateriële gevolgen, maar ook tot materiele gevolgen.
De melding stelt de betrokkene in staat om alert te zijn op de mogelijke gevolgen van het datalek en om zich daar waar mogelijk tegen te wapenen door, bijvoorbeeld, een gelekt wachtwoord te vervangen. De wet schrijft voor dat de melding onverwijld wordt gedaan. Er moet daarbij rekening worden gehouden met het feit dat de betrokkene naar aanleiding van de melding mogelijk maatregelen moet nemen om zich te beschermen tegen de gevolgen van het datalek. Hoe eerder we de betrokkene daarover informeren, hoe eerder deze in actie kan komen.
Als er passende technische beschermingsmaatregelen zijn genomen waardoor de persoonsgegevens die het betreft onbegrijpelijk of ontoegankelijk zijn voor onbevoegden, dan kan de melding aan de betrokkene achterwege laten. Bij deze beschermingsmaatregelen moeten we bijvoorbeeld denken aan cryptografische bewerkingen zoals encryptie en hashing. Er moet per geval worden bepaald of de maatregelen die er zijn genomen voldoende bescherming bieden om de melding aan de betrokkene achterwege te kunnen laten.

5. Afhandeling na datalek

Vraag:
Welke vervolgacties moeten nog worden uitgezet ter afhandeling van het incident. Denk aan:

- opname in het overzicht van datalekken dat PCBO moet voeren:

Bewaarplicht bij een datalek
In het geval van een datalek geldt een bewaarplicht die is vastgelegd in artikel 34a lid 8 Wbp: ''De verantwoordelijke houdt een overzicht bij van iedere inbreuk die leidt tot de aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens. Het overzicht bevat in ieder geval feiten en gegevens omtrent de aard van de inbreuk, bedoeld in het derde lid, alsmede de tekst van de kennisgeving aan de betrokkene.''

Documenten die in ieder geval moeten worden bewaard nadat zich een datalek heeft voorgedaan:
1. Feiten en gegevens omtrent de aard van de inbreuk;
2. De tekst van de kennisgeving aan betrokkenen;
3. De melding zoals die is ingediend bij de AP.

Aanvullend verdient het aanbeveling bij het overzicht ook de volgende documenten te bewaren:
4. Meest recente actielijst van de genomen processtappen;
5. Eventuele aansprakelijkheidsstellingen en klachten;
6. Overige correspondentie voor zover van belang

Het overzicht behoeft niet openbaar te worden gemaakt.

- afhandeling mogelijke klachten en/of aansprakelijkheidsstellingen
- uitzoeken wie precies verantwoordelijk en aansprakelijkheidsstelling
- communicatie extern/intern

Nadere uitwerking en bijlagen volgen in 2018-2019.