2018

Datalekprotocol 2018 & Invalprotocol

Deze protocollen zijn met de grootst mogelijk zorgvuldigheid opgesteld door Rosalie de Groen en Dennis van Iterson van Triplepro Online Marketing BV. U kunt aan deze audit geen rechten ontlenen. Wel kunnen wij u verder adviseren welke organisatorische maatregelen u kunt treffen om te voldoen aan de wetgeving omtrent uw diensten. De AVG is op een aantal onderdelen niet altijd even duidelijk, waardoor niet tot in detail kan worden bepaald wat er op dit moment van een onderneming wordt verwacht om aan de nieuwe privacywetgeving te voldoen. Het hebben en naleven van deze twee protocollen is verplicht. Voordat een onderneming concrete actie onderneemt naar aanleiding van deze audit wordt geadviseerd om juridische bijstand in te schakelen.

Zorg ervoor dat bij het verzamelen en verwerken van persoonsgegevens niet meer gegevens worden gebruikt dan nodig is om het doel, waarvoor ze gebruikt zullen worden, te bereiken. Zorg dus voor dataminimalisatie.

Inhoudsopgave

Datalekprotocol 2018

Waarom dit protocol

In dit datalekprotocol van <……..> staat beschreven hoe er binnen <……..> wordt omgegaan met datalekken. Het is goed te weten dat wij eigenaar zijn van onze personeelsgegevens en klantgegevens, echter enkel verwerker zijn van de gegevens van klanten van onze klanten. Onderstaand is omschreven hoe gezorgd wordt voor het adequaat informeren van de betrokkenen. Voor medewerkers van <……..> geldt: wees transparant en vertel wat er is gebeurd. Leg uit wat er is gedaan om een hack te voorkomen, geef aan als het ondanks de beveiliging toch is misgegaan. Is er bijvoorbeeld een geavanceerde hack geweest waartegen de beveiliging niet was opgewassen, geef dit dan toe. Bied namens <……..> je excuses aan en leg uit dat er wordt gewerkt aan een betere beveiliging. Geef in heldere taal aan welke stappen de betrokkenen zelf kunnen nemen om de schade zo beperkt mogelijk te houden, raad hen bijvoorbeeld aan om alle wachtwoorden te wijzigen. Bied de gedupeerden tevens, waar nodig, iets extra's aan. Denk hierbij aan een rechtstreeks telefoonnummer waar ze terecht kunnen met vragen.

Logboek

Vanaf het moment dat er een datalek geconstateerd is zullen we een logboek datalekken bijhouden, deze moet bevatten:

1. een korte omschrijving van het lek;
2. wanneer het lek plaatsvond;
3. wat er met de gegevens is gebeurd (zijn ze verloren gegaan, door onbevoegden ingezien, gekopieerd of gewijzigd);
4. van welke groepen personen gegevens zijn gelekt en om hoeveel personen het gaat;
5. om welke soort(en) gegevens het gaat;
6. de instanties waar meer informatie over de inbreuk kan worden verkregen;
7. de aanbevolen maatregelen om de negatieve gevolgen van de inbreuk te beperken (bijvoorbeeld: het veranderen van gebruikersnamen en wachtwoorden);
8. een beschrijving van de geconstateerde en de vermoedelijke gevolgen van de inbreuk voor de verwerking van persoonsgegevens;
9. de maatregelen die de organisatie heeft genomen of voorstelt te nemen om deze gevolgen te verhelpen en in de toekomst te voorkomen;
10. hoe en wat er wanneer is gecommuniceerd met de betrokken externen.

Het protocol

Stap 1 Melding directie

Zodra een datalek geconstateerd wordt, moet deze binnen 4 uur worden gemeld bij de opdrachtgever. Deze zal vervolgens bepalen welke stappen genomen zullen worden om de schade te beperken. In het geval van een datalek met klantgegevens zal <……..> deze verantwoordelijkheid direct verleggen naar de eigenaar van de gegevens en hier binnen 4uur melding van maken bij de betreffende organisatie. In dit geval zijn stap 2 en 3 niet van toepassing dan wel niet aan <……..> om uit te voeren.

Stap 2 Bepalen of een melding noodzakelijk is

De Directie bepaalt het ‘risicocriterium’. (Een datalek zal altijd gemeld worden bij de betreffende opdrachtgever.) Ter illustratie: als er sprake is van een inbreuk, bekijkt de wetgever of er een aanmerkelijk risico is dat persoonsgegevens zijn verloren of onrechtmatig worden verwerkt. Hierbij wegen zij alle omstandigheden van het geval mee. Hoe het risicocriterium in de praktijk wordt toegepast is (nog niet) duidelijk. De wetgever noemt als voorbeeld het zoekraken van de ledenadministratie van een sportvereniging. De gevolgen voor de leden blijven daarbij meestal beperkt, zodat een melding niet nodig is. Bij de Belastingdienst ligt dat uiteraard heel anders. Bij de AVG geldt dat u als verantwoordelijke alle gevallen meldt waarbij sprake is van inbreuk op persoonsgegevens.

Stap 3 Autoriteit Persoonsgegevens informeren

<……> zal melding maken bij het Autoriteit Persoonsgegevens.

Stap 4 Informeer de betrokkenen

Door de betrokkenen en de kring van betrokkenen snel en adequaat te informeren over het datalek, verkleinen wij de kans op ontevreden personeel of klanten. Ook de aard van de inbreuk en de gevolgen daarvan voor de verwerking van persoonsgegevens spelen een belangrijke rol in de communicatiekeuzes die wij maken. Zo kan er gekozen worden voor bijvoorbeeld een persoonlijk bericht, een bericht op een website. Het is in ieder geval belangrijk om bij (grootschalige) datalekken zelf contact op te nemen met de pers en ze te informeren over wat er is gebeurd. Hier ligt een rol voor de persvoorlichter of woordvoerder die namens de organisatie spreekt. Onderstaand staat omschreven hoe <……> zorg kan dragen voor het adequaat informeren van de betrokkenen: • wees transparant en vertel wat er is gebeurd; • leg uit wat er is gedaan om een hack te voorkomen; • vertel dat het ondanks de beveiliging toch is misgegaan; • wees open als het bijvoorbeeld een geavanceerde hack was waartegen de beveiliging niet was opgewassen; • bied excuses aan en leg uit dat wordt gewerkt aan een betere beveiliging; • geef in heldere taal aan welke stappen de betrokkenen zelf kunnen nemen om de schade zo beperkt mogelijk te houden; • raad hen bijvoorbeeld aan om wachtwoorden te wijzigen; • bied de gedupeerden, waar nodig, iets extra’s aan. Denk hierbij aan een rechtstreeks nummer waar ze terecht kunnen met vragen.

Invalprotocol

Protocol ongepland bezoek door toezichthouders

Bellijst:

<.....> (Functionaris Gegevenbescherming): 0612345678
<.....> (Technisch Directeur): 0612345678
<.....> (Algemeen Directeur): 0612345678

Er bestaat een reële kans dat <.....> gecontroleerd wordt door een toezichthouder. In dit document zetten we uiteen hoe eenieder moet handelen in geval van een al dan niet aangekondigde controle.

In het kader van hun toezicht hebben de autoriteiten (bijvoorbeeld Autoriteit Persoonsgegevens) de bevoegdheid om onaangekondigde bedrijfsbezoeken uit te voeren. Dergelijke bedrijfsbezoeken zijn vaak het gevolg van klachten, maar kunnen ook plaatsvinden op eigen initiatief van de toezichthouder. Bij een dergelijk bezoek zal de toezichthouder willen nagaan of de wet- en regelgeving voldoende wordt nageleefd. Er zal informatie worden vergaard, die later als basis kan dienen voor een mogelijk sanctiebesluit.

Omdat de bedrijfsbezoeken vrijwel altijd onaangekondigd plaatsvinden is het van groot belang om daarop goed voorbereid te zijn. Hieronder zal een aantal belangrijke aandachtspunten worden weergegeven.

Aandachtspunten bij een bedrijfsbezoek

Aankomst van de ambtenaren

De ambtenaren melden van welke instantie ze zijn. Autoriteit Persoonsgegevens (AP) is een toezichthouder op het gebied van privacy die ons mag controleren. Daarnaast is de FIOD op fiscaal gebied een toezichthouder die bevoegd is om te controleren. Wanneer er ambtenaren van een andere instantie zijn dan hoef je deze niet binnen te laten.

• Begeleid de ambtenaren onmiddellijk naar een aparte ruimte, waarin zich geen relevante informatie bevindt.

• Vraag naar de identificatiegegevens van de ambtenaren en vraag wat het doel en de grondslag van het onderzoek is. Vraag om een schriftelijke bevestiging.

• Neem direct contact op met de Directie en vraag de ambtenaren te wachten tot de komst van de Directie. Normaliter zijn de ambtenaren bereid 30- 45 minuten te wachten.

• De ambtenaren hebben in beginsel de bevoegdheid bedrijfspanden, terreinen en vervoersmiddelen te betreden. Onder omstandigheden mogen zij ook woningen van directeuren, bestuurders en andere personeelsleden onderzoeken. Voor deze bevoegdheid hebben de ambtenaren een voorafgaande machtiging nodig van een rechter-commissaris.

• Zorg ervoor dat iedere ambtenaar te allen tijde wordt vergezeld en dat voorkomen wordt dat ambtenaren alleen rondlopen.

• Vraag de ambtenaar waarom de toegang tot een bepaalde ruimte vereist is. Noteer hun antwoorden.

Inzage en kopieën

• De ambtenaren hebben de bevoegdheid om zowel analoge als digitale informatie in te zien. Een uitzondering geldt voor: privé-documenten, documenten die redelijkerwijs niet relevant zijn voor het doel van het onderzoek, en geprivilegieerde correspondentie tussen de onderneming en een externe advocaat. Maak bezwaar tegen de inzage van dergelijke informatie en maak hier een notitie van.

• De ambtenaren hebben de bevoegdheid om van de gegevens en bescheiden kopieën te (laten) maken. Noteer van welke informatie kopieën worden meegenomen en maak ook eigen kopieën. Voor digitale gegevens gelden specifieke regels.

• Onder geen beding dient een poging te worden ondernomen om (digitale) documenten, boeken en bescheiden waarvan ambtenaren inzage vragen te verstoppen of te vernietigen, dan wel om ambtenaren te misleiden omtrent het bestaan of de inhoud van (digitale) documenten, boeken en bescheiden waar door de ambtenaren om wordt verzocht. Voor dergelijk handelen kunnen hoge boetes worden opgelegd aan de onderneming en eventueel aan de individuen.

• Wanneer het onderzoek niet binnen een dag kan worden afgerond hebben de ambtenaren de bevoegdheid om bedrijfsruimten of voorwerpen te verzegelen. Het is verboden de afgesloten ruimtes te betreden.

• Er moet te allen tijde voorkomen worden dat een zegel wordt verbroken; daarvoor kunnen zeer omvangrijke boetes worden opgelegd. Instrueer de werknemers (waaronder relevante derde partijen zoals het schoonmaakbedrijf) verzegelde ruimtes niet te betreden.

Verhoor

• De ambtenaren kunnen tijdens het bedrijfsbezoek om inlichtingen vragen. Hieronder valt ook het horen van personen die betrokken zijn bij de onderneming.

• Laat het verhoor alleen plaatsvinden in aanwezigheid van de directie.

• Controleer of de ambtenaren de te horen personen wijzen op het recht te zwijgen en (de zogenaamde ‘cautie’) hebben medegedeeld.

• Beantwoord géén vragen waarbij men zichzelf of de onderneming zou beschuldigen (van het overtreden van wet- en regelgeving).

• Beantwoord geen onduidelijke vragen, verzoek de ambtenaar de vraag anders te formuleren en, indien nodig, schriftelijk te stellen.

• Beantwoord alleen de gestelde vraag en geef niet vrijwillig extra informatie.

• Indien er geen volledig of juist antwoord gegeven kan worden, verzoek de ambtenaar dan het antwoord op een later moment schriftelijk te mogen verstrekken. Geef onder geen beding een onvolledig of onjuist antwoord.

• Er wordt een uitgewerkte versie van de afgelegde verklaring door de ACM verstrekt, waarin de door de ambtenaren gestelde vragen en daarop gegeven antwoorden zijn weergegeven. Controleer deze verklaring en indien hier onjuistheden in staan ondertekent u het niet.

Na afloop van het onderzoek

• Vraag de contactgegevens van de ambtenaar van de toezichthouder die de zaak zal behandelen.

• Vraag de ambtenaren om een kopie van het verslag dat zij tijdens het bezoek hebben gemaakt en vraag om een kopie van het door hen gemaakte overzicht van de documenten die zij hebben ingezien en gekopieerd.

• Begeleid de ambtenaren naar de uitgang van het gebouw. Maak een eigen verslag van het precieze verloop van het bedrijfsbezoek, inclusief de mogelijke incidenten die zich daarbij hebben voorgedaan.

• Organiseer een bijeenkomst met alle betrokken personen en de Directie om te bepalen welke acties nog ondernomen dienen te worden.

• Stel beleid vast voor externe communicatie, bijvoorbeeld het op de hoogte stellen van de klanten wiens gegevens het betreft.