Protocol beveiligingsincidenten en datalekken

van

Easysource

1. Inleiding

Het Protocol biedt een handleiding voor de melding, beoordeling en afhandeling van beveiligingsincidenten en datalekken. Het Protocol is een bijlage bij het gegevensbeschermingsbeleid. Evaluatie vindt plaats op de daarin beschreven wijze.

2. Definities

In het Protocol worden de hiernavolgende definities gehanteerd:

AVG: verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming);

AP: Autoriteit Persoonsgegevens;

beveiligingsincident: een inbreuk op de beveiliging, waardoor persoonsgegevens worden vernietigd, verloren gaan, gewijzigd worden, ongeoorloofd worden verstrekt aan derden, of derden ongeoorloofd toegang hebben (gehad) tot persoonsgegevens;

beveiligingsincidentenregister: het register zoals bedoeld in art. 33 lid 5 AVG;

datalek: een inbreuk als bedoeld in art. 33 en/of art. 34 AVG dat gemeld moet worden aan de AP en/of aan de betrokkenen;

Easysource: de vennootschap onder firma **Easysource**, gevestigd te (6443 AG) Brunssum aan de Prins Hendriklaan 416, ingeschreven in het handelsregister van de Kamer van Koophandel onder nummer 63952483;

gegevensbeschermingsbeleid: het binnen Easysource geldende gegevensbeschermingsbeleid;

meldplicht datalekken: de verplichtingen zoals opgenomen in art. 33 en 34 AVG;

Protocol: het onderhavige document.

3. Achtergrond en doel van het Protocol

Het Protocol is opgesteld met het doel om personen binnen Easysource te informeren en bewustwording te creëren over de meldplicht datalekken. Deze meldplicht is opgenomen in art. 33 en 34 AVG. Onder omstandigheden is het bij een datalek nodig om de toezichthouder - de AP - en eventueel ook de betrokkenen te informeren over het feit dat een datalek heeft plaatsgevonden.

Het is belangrijk dat personen binnen Easysource kennis van de meldplicht datalekken hebben, omdat een datalek vaak gepaard gaat met ingrijpende gevolgen voor de betrokkenen (personen van wie de gegevens gelekt zijn). Het Protocol maakt daarnaast duidelijk dat niet alle beveiligingsincidenten kwalificeren als een datalek dat gemeld moet worden aan de toezichthouder en/of de betrokkenen. Voor Easysource is het van belang dat bij beveiligingsincidenten en datalekken duidelijk is hoe moet worden gehandeld.

4. Stappenplan meldplicht datalekken

4.1. Toelichting onderscheid beveiligingsincident en datalek

Van belang is om een onderscheid te maken tussen een beveiligingsincident en een datalek. De wet noemt een beveiligingsincident formeel een "inbreuk op de beveiliging" en definieert dat als 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*"

Je kunt bij een beveiligingsincident bijvoorbeeld denken aan de volgende gevallen:

- een kwijtgeraakte USB-stick;
- een hack;
- een geslaagde ransomware-aanval;
- het versturen van een bestand met persoonsgegevens aan een persoon waarvoor het niet bedoeld is;
- het converteren van een bestand met persoonsgegevens via een online tool;

- het verstrekken van wachtwoorden aan personen waarvoor het niet bedoeld is;
- het onbeheerd achterlaten van een onbeveiligde computer in een publieke ruimte;
- het versturen van een brief met gevoelige gegevens aan de verkeerde persoon;
- voor het publiek toegankelijke kast met personeelsdossiers.

Ieder beveiligingsincident wordt intern gemeld bij de daarvoor binnen Easysource verantwoordelijke persoon (het interne meldpunt). Hoe dat concreet in zijn werk gaan, wordt verderop in het Protocol uitgelegd.

Niet ieder beveiligingsincident is echter een datalek. Een datalek is namelijk een beveiligingsincident dat daadwerkelijk een risico oplevert voor de personen van wie de persoonsgegevens gelekt zijn. Denk aan een risico op identiteitsfraude. Een dergelijk risico is niet bij alle beveiligingsincidenten aanwezig. Dat kan zijn omdat de persoonsgegevens goed beveiligd zijn of omdat de impact van het beveiligingsincident erg klein is. In die gevallen hoeft een beveiligingsincident (meestal) niet gemeld te worden aan de toezichthouder of aan de personen van wie de persoonsgegevens gelekt zijn. Als geen melding verricht hoeft te worden, is juridisch gezien geen sprake van een datalek.

Doel van het Protocol is dat alle door de personen opgemerkte beveiligingsincidenten intern worden gemeld. Het doen van een externe melding is nooit toegestaan. Na de interne melding wordt door Easysource beoordeeld of het beveiligingsincident daadwerkelijk kwalificeert als een datalek (en extern gemeld moet worden).

4.2. Stap 1: Ontdekken van een beveiligingsincident

Bij het succesvol behandelen en afhandelen van een beveiligingsincident zijn diverse personen betrokken. De belangrijkste daarvan zijn:

1. **de ontdekker**: de persoon die mogelijk een beveiligingsincident ontdekt en de procedure zoals opgenomen in dit Protocol volgt;
2. **het interne meldpunt**: het interne meldpunt waar beveiligingsincidenten worden gemeld;

Als de ontdekker denkt dat sprake is van een beveiligingsincident, dan meldt zich hij of zij dit direct en zo snel mogelijk bij het interne meldpunt: de heer S.

Montie, op werkdagen op telefoonnummer 045-5273575 en ook per e-mail op het e-mailadres kantoor@easysource.nl. Daarbij wordt de volgende informatie doorgegeven:

- samenvatting van het beveiligingsincident;
- voor zover de ontdekker dit kan overzien: de waarschijnlijke gevolgen van het beveiligingsincident;
- welke (persoons)gegevens bij het beveiligingsincident zijn betrokken;
- wanneer het beveiligingsincident vermoedelijk heeft plaatsgevonden;
- voor zover de ontdekker dit kan overzien: welke maatregelen zouden moeten worden genomen om de gevolgen van het beveiligingsincident te beperken;
- alle andere informatie welke de ontdekker van belang acht.

Belangrijk: Wij ontvangen liever (veel) teveel interne meldingen, dan te weinig. Schroom dus niet om een interne melding te verrichten en wees daarbij zo volledig en eerlijk mogelijk. Zonder nader overleg met het meldpunt neemt de ontdekker geen maatregelen en verricht de ontdekker geen (externe) meldingen.

4.3. Stap 2: Inventarisatie van het beveiligingsincident

Na een melding van de ontdekker, bepaalt het interne meldpunt direct en zo snel mogelijk of er voldoende informatie over het beveiligingsincident beschikbaar is om Stap 3 uit te kunnen voeren (juridische beoordeling van het beveiligingsincident en nemen maatregelen). Zo niet, dan kan het interne meldpunt aanvullende vragen aan de ontdekker stellen. In dit stadium verzamelt het interne meldpunt ook zoveel als mogelijk technische informatie. Om die reden wordt mogelijk de hulp ingeschakeld van personen met een expertise op het gebied van informatiebeveiliging.

4.4. Stap 3: Juridische beoordeling van het beveiligingsincident en nemen maatregelen

Na de inventarisatie van het beveiligingsincident, beoordeelt het interne meldpunt of het beveiligingsincident in juridische zin kwalificeert als een datalek. Omdat het hier om een juridische beoordeling gaat, zal het interne meldpunt dit in eigenlijk alle gevallen met een jurist beoordelen.

Tegelijkertijd neemt het interne meldpunt alle noodzakelijke maatregelen om (de gevolgen van) het beveiligingsincident aan te pakken en om (verdere) schade of nadelige gevolgen te voorkomen. De genomen en te nemen maatregelen worden gedocumenteerd en vastgelegd in het beveiligingsincidentenregister (Stap 6).

Hierna is – voor de achtergrond – de wettekst van de meldplicht datalekken opgenomen.

Artikel 33

Melding van een inbreuk in verband met persoonsgegevens aan de toezichthoudende autoriteit

1. *Indien een inbreuk in verband met persoonsgegevens heeft plaatsgevonden, meldt de verwerkingsverantwoordelijke deze zonder onredelijke vertraging en, indien mogelijk, uiterlijk 72 uur nadat hij er kennis van heeft genomen, aan de overeenkomstig artikel 55 bevoegde toezichthoudende autoriteit, tenzij het niet waarschijnlijk is dat de inbreuk in verband met persoonsgegevens een risico inhoudt voor de rechten en vrijheden van natuurlijke personen. Indien de melding aan de toezichthoudende autoriteit niet binnen 72 uur plaatsvindt, gaat zij vergezeld van een motivering voor de vertraging.*

2. *De verwerker informeert de verwerkingsverantwoordelijke zonder onredelijke vertraging zodra hij kennis heeft genomen van een inbreuk in verband met persoonsgegevens.*

3. *In de in lid 1 bedoelde melding wordt ten minste het volgende omschreven of meegedeeld:*

   a) *de aard van de inbreuk in verband met persoonsgegevens, waar mogelijk onder vermelding van de categorieën van betrokkenen en persoonsgegevensregisters in kwestie en, bij benadering, het aantal betrokkenen en persoonsgegevensregisters in kwestie;*

   b) *de naam en de contactgegevens van de functionaris voor gegevensbescherming of een ander contactpunt waar meer informatie kan worden verkregen;*

   c) *de waarschijnlijke gevolgen van de inbreuk in verband met persoonsgegevens;*

   d) *de maatregelen die de verwerkingsverantwoordelijke heeft voorgesteld of genomen om de inbreuk in verband met persoonsgegevens aan te pakken, waaronder, in voorkomend geval, de maatregelen ter beperking van de eventuele nadelige gevolgen daarvan.*

4. *Indien en voor zover het niet mogelijk is om alle informatie gelijktijdig te verstrekken, kan de informatie zonder onredelijke vertraging in stappen worden verstrekt.*

5. *De verwerkingsverantwoordelijke documenteert alle inbreuken in verband met persoonsgegevens, met inbegrip van de feiten omtrent de inbreuk in verband met persoonsgegevens, de gevolgen daarvan en de genomen corrigerende maatregelen. Die documentatie stelt de toezichthoudende autoriteit in staat de naleving van dit artikel te controleren.*

Artikel 34

Mededeling van een inbreuk in verband met persoonsgegevens aan de betrokkene

1. *Wanneer de inbreuk in verband met persoonsgegevens waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen, deelt de verwerkingsverantwoordelijke de betrokkene de inbreuk in verband met persoonsgegevens onverwijld mee.*

2. *De in lid 1 van dit artikel bedoelde mededeling aan de betrokkene bevat een omschrijving, in duidelijke en eenvoudige taal, van de aard van de inbreuk in verband met persoonsgegevens en ten minste de in artikel 33, lid 3, onder b), c) en d), bedoelde gegevens en maatregelen.*

3. *De in lid 1 bedoelde mededeling aan de betrokkene is niet vereist wanneer een van de volgende voorwaarden is vervuld:*

    a) *de verwerkingsverantwoordelijke heeft passende technische en organisatorische beschermingsmaatregelen genomen en deze maatregelen zijn toegepast op de persoonsgegevens waarop de inbreuk in verband met persoonsgegevens betrekking heeft, met name die welke de persoonsgegevens onbegrijpelijk maken voor onbevoegden, zoals versleuteling;*

    b) *de verwerkingsverantwoordelijke heeft achteraf maatregelen genomen om ervoor te zorgen dat het in lid 1 bedoelde hoge risico voor de rechten en vrijheden van betrokkenen zich waarschijnlijk niet meer zal voordoen;*

    c) *de mededeling zou onevenredige inspanningen vergen. In dat geval komt er in de plaats daarvan een openbare mededeling of een soortgelijke maatregel waarbij betrokkenen even doeltreffend worden geïnformeerd.*

4. *Indien de verwerkingsverantwoordelijke de inbreuk in verband met persoonsgegevens nog niet aan de betrokkene heeft gemeld, kan de toezichthoudende autoriteit, na beraad over de kans dat de inbreuk in verband met persoonsgegevens een hoog risico met zich meebrengt, de verwerkingsverantwoordelijke daartoe verplichten of besluiten dat aan een van de in lid 3 bedoelde voorwaarden is voldaan.*

4.5. Stap 4: Verrichten melding aan AP en/of betrokkenen

Indien sprake is van een datalek dat gemeld moet worden aan de AP en/of betrokkenen, dan worden de betreffende meldingen verricht. Het uitgangspunt van de wet is dat de melding binnen 72 uur na de ontdekking (Stap 1) moet plaatsvinden. Een melding aan de AP kan verricht worden via de website https://datalekken.autoriteitpersoonsgegevens.nl/.
Niet iedere datalek dat gemeld moet worden aan de AP hoeft overigens aan de betrokkenen gemeld te worden. In Stap 3 is beoordeeld of het datalek ook aan de betrokkenen gemeld moet worden.

4.6. Stap 5: Nemen van nadere maatregelen

Na de melding aan de AP en/of de betrokkenen, neemt het interne meldpunt (indien nodig) nadere maatregelen om het datalek te repareren, om vergelijkbare beveiligingsincidenten in de toekomst te voorkomen, om (verdere) schade te voorkomen en/of om nadelige gevolgen te voorkomen. De genomen maatregelen worden gedocumenteerd en vastgelegd in het beveiligingsincidentenregister (Stap 6).

4.7. Stap 6: Beveiligingsincidentenregister

Alle beveiligingsincidenten, of deze nou gemeld zijn aan de AP en/of de betrokkenen of niet, worden gedocumenteerd in het beveiligingsincidentenregister. In dat register is de volgende informatie opgenomen:

- de feiten van de beveiligingsincidenten;
- de gevolgen van de beveiligingsincidenten;
- de genomen maatregelen als gevolg van de beveiligingsincidenten.

Het beveiligingsincidentenregister wordt op verzoek beschikbaar gesteld aan de AP.