Protocol Datalekken

Dit protocol beschrijft de procedure met daarin te nemen maatregelen die binnen dispi en denq (bewerker) genomen moeten worden bij een datalek volgens de meldplicht datalekken van de Wet bescherming persoonsgegevens (Wbp). De meldplicht datalekken is een wijziging van de Wbp waarbij artikel 34a aan die wet is toegevoegd en treedt in werking met ingang van 1 januari 2016.

Begrippen

Licentiehouder : de relatie van dispi die een licentie e-Captain in gebruik heeft conform de overeenkomst
Bewerker : dispi, ontwikkelaar van e-Captain en contracthouder
Datalek : onbedoelde of onwettige vernietiging, verlies of wijziging van, of een niet geautoriseerde toegang tot verwerkte persoonsgegevens

Reikwijdte van de meldplicht datalekken
Indien er sprake is van een inbreuk op de beveiliging van persoonsgegevens als bedoeld in artikel 13 van Wbp die leidt tot een aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens van de licentiehouder, dan wordt dit als een datalek gekwalificeerd en zal dit bij de Autoriteit Persoons-gegevens moeten worden gemeld. Er moet sprake zijn van het 'lekken van data' en dat het lekken een onbedoelde of onwettige vernietiging, verlies of wijziging van, of een niet geautoriseerde toegang tot verwerkte persoonsgegevens tot gevolg heeft.
Een enkele tekortkoming of kwetsbaarheid in de beveiliging is geen datalek tenzij dit leid tot een onrechtmatige verwerking.

Datalekken kunnen ontstaan door:

- moedwillig handelen (cybercriminaliteit, hacking, identiteitsfraude, mailware besmetting);
- technisch falen (ICT-storingen);
- menselijk falen (het verstrekken van username/wachtwoord aan collega’s en externen);
- calamiteit (brand datacentrum, wateroverlast);
- verloren USB stick of laptop;
- verzenden van email met emailadressen van alle geadresseerden;

Meldingen
Een datalek kan door een medewerker van de bewerker of een licentiehouder van e-Captain worden ontdekt. Deze ontdekking wordt aan de licentiehouder en bij diens afwezigheid aan de directie van de bewerker medegedeeld die vervolgens over zal gaan tot de beoordeling of er sprake is van een datalek. Het bestuur / directie onderzoekt het incident. Hierbij is aandacht voor de volgende aspecten: De bewerker is degene die de gegevens ten behoeve van de licentiehouder verwerkt zonder aan haar rechtstreeks gezag te zijn onderworpen (ook extern). De bewerker verwerkt persoonsgegevens overeenkomstig de instructies en uiteindelijke verantwoordelijkheid van de licentiehouder. De bewerker zal de licentiehouder tijdig en adequaat informeren over relevante incidenten.

- a. wat is de aard van het datalek (bijzondere of gevoelige gegevens dienen per definitie te worden gemeld) ;
- b. wat is de oorzaak dat dit incident heeft plaatsgevonden;
- c. is er sprake van het niet nakomen van of een tekortkoming in de beveiligingsprocedures;
- d. is de organisatie verwijtbaar.

Indien sprake is van een datalek dan zal de licentiehouder binnen 2 dagen maar niet later dan 72 uur na ontdekking zorg dragen voor een melding bij de Autoriteit Persoonsgegevens. Verder zal de licentiehouder een overzicht bijhouden van alle datalekken binnen de eigen organisatie.

Per datalek wordt in het overzicht aangegeven wat de feiten en gegevens zijn van de aard van de inbreuk. Een datalek wordt voor minimaal 1 jaar in het overzicht bewaard.
Na de melding datalek ontvangt de licentiehouder een ontvangstbevestiging van de Autoriteit Persoonsgegevens. De Autoriteit Persoonsgegevens zal contact met de licentiehouder opnemen mocht na een melding aanleiding zijn om nadere stappen te ondernemen. Hierbij zal met name de herkomst van de melding worden geverifieerd en kan de licentiehouder aanwijzingen van de Autoriteit Persoonsgegevens krijgen.
Wanneer vaststaat dat een datalek bij de Autoriteit Persoonsgegevens gemeld moet worden dan dient hierna beoordeeld te worden of een datalek ook aan betrokkene moet worden gemeld. Betrokkenen zijn degenen wiens persoonsgegevens zijn betrokken bij een inbreuk. In het geval van de licentiehouder zijn de betrokkenen over het algemeen de leden / donateurs, en ondernemingen die sponsoren, adverteren of producten afnemen.

Een betrokkene moet ook onverwijld in kennis worden gesteld van de inbreuk. Indien de inbreuk waarschijnlijk geen ongunstige gevolgen zal hebben voor de persoonlijke levenssfeer van de betrokkene of wanneer de technische beschermingsmaatregelen (bijvoorbeeld encryptie) die zijn genomen voldoende bescherming bieden, kan melding van het datalek aan de betrokkene achterwege blijven.

Taken, verantwoordelijkheden en bevoegdheden

1. Iedere medewerker van de licentiehouder die direct of indirect kennis draagt of krijgt van een datalek, is verplicht dit direct te melden aan het bestuur/directie van de licentiehouder;
2. De licentiehouder is verantwoordelijk voor het onderzoeken van het incident;
3. De licentiehouder is verantwoordelijk voor de beoordeling of een datalek aan de Autoriteit Persoonsgegevens gemeld moet worden respectievelijk of een datalek aan de betrokkene moet worden gemeld;
4. De licentiehouder is verantwoordelijk voor de melding van datalekken bij de Autoriteit Persoonsgegevens;
5. De licentiehouder is verantwoordelijk voor het bijhouden van een overzicht van alle datalekken die onder de meldplicht vallen voor minimaal 1 jaar;
6. De licentiehouder is verantwoordelijk voor het ondernemen van preventieve, reparatoire en repressieve maatregelen.

Interne controle

1. De medewerker systeembeheer analyseert jaarlijks de meldingen datalekken en stelt indien nodig een verbeterplan ter voorkoming van datalekken.

2. Het bestuur/directie beoordeelt minimaal jaarlijks of de procedure en de uitvoering van dit protocol nog met elkaar in overeenstemming zijn. Indien deze niet met elkaar overeenkomen wordt beoordeeld of de procedure geactualiseerd moet worden of dat medewerkers geïnstrueerd moeten worden op een juiste toepassing van de protocol.