Datalek

1. Protocol informatiebeveiligingsincidenten en datalekken

Betreffende het protocol sluiten wij ons aan bij het protocol informatiebeveiligingsincidenten en datalekken van HLTsamen.
Dit protocol biedt een handleiding voor de melding, beoordeling en afhandeling van informatiebeveiligingsincidenten en datalekken. Het doel hiervan is het op juiste wijze in behandeling nemen en afwikkelen van ontstane incidenten en datalekken.

2. Gebruikte termen:

- Informatievoorziening: het geheel van mensen, middelen en maatregelen, gericht op de informatiebehoefte van de organisatie.
- Beveiligingsincident: een gebeurtenis die ervoor zorgt of zou kunnen zorgen dat de beschikbaarheid, integriteit en/of vertrouwelijkheid van de informatievoorziening wordt aangetast.
- Datalek: een beveiligingsincident waarbij persoonsgegevens verloren raken of onrechtmatig worden verwerkt (opgeslagen, aangepast, verzonden, et cetera).
- Betrokkene: de persoon op wie de persoonsgegevens betrekking hebben, degene van wie de gegevens worden verwerkt.

3. Wet- en regelgeving

Met ingang van 25 mei 2018 is de Algemene Verordening Gegevensbescherming (AVG) in werking getreden, die een meldplicht voor ernstige datalekken regelt. De AVG stelt strenge eisen aan de registratie van datalekken. Organisaties zijn verplicht om alle datalekken te documenteren. Met deze documentatie kan de Autoriteit Persoonsgegevens (hierna: AP) controleren of aan de meldplicht is voldaan. Ernstige datalekken moeten gemeld worden aan de AP en - in bepaalde situaties - ook aan de betrokkene(n).

De meldplicht voor gemeenten ligt bij de bestuursorganen, zoals het college van B&W, de gemeenteraad en de burgemeester, maar ook de Rekenkamer. Zij zijn eindverantwoordelijk voor de verwerking van persoonsgegevens. Met leveranciers worden afspraken gemaakt over het melden van datalekken in een verwerkersovereenkomst.

Als er sprake is van een ernstig datalek, moet er binnen 72 uur na ontdekking van het lek een melding bij de AP worden gedaan.

4. Werkwijze

4.1. Uitgangssituatie

- Er is een actueel informatiebeveiligingsbeleid en privacybeleid
- Er is een actueel document betreffende het aanvaardbaar gebruik van bedrijfsmiddelen (door middel van bijvoorbeeld een bruikleenovereenkomst voor laptop of telefoon) en/of Gedragscode werkorganisatie HLTsamen.

4.2. Drie rollen

Er zijn tenminste drie verschillende rollen nodig die een beveiligingsincident en/of datalek succesvol kunnen afhandelen:

- Ontdekker (medewerker of inwoner); degene die het beveiligingsincident of datalek op het spoor komt en het proces in werking stelt.
- Meldpunt (via Topdesk); hier worden alle beveiligingsincidenten en datalekken geregistreerd. Het Meldpunt bestaat uit de Chief Information Security Officer (CISO), de Functionaris Gegevensbescherming (FG) en de Privacy Officer (PO).

- Technicus (systeembeheer); degene die de (eventueel) technische oorzaak van het datalek kan vinden en kan (laten) repareren.

5. Zeven stappen

Hieronder staan de zeven stappen die doorlopen worden, vanaf het moment van ontdekking van een beveiligingsincident tot het informeren van betrokkenen.

5.1. Ontdekken

De Ontdekker merkt een beveiligingsincident op, via eigen waarneming, of via waarneming van een derde. De Ontdekker (inwoner) meldt een beveiligingsincident via een speciaal daarvoor aangemaakt e-mailadres en geeft daarbij zoveel mogelijk beschikbare informatie door. De Ontdekker (medewerker) meldt een beveiligingsincident in Topdesk en geeft daarbij zoveel mogelijk beschikbare informatie door.

5.2. Inventariseren

Na de melding bepaalt het Meldpunt of er voldoende informatie over het beveiligingsincident bekend is. Zo niet, dan zet het Meldpunt aanvullende vragen uit bij de Ontdekker en/of de Technicus.
De volgende informatie wordt vastgelegd als er sprake is van een beveiligingsincident:

- Aard van het beveiligingsincident
- Samenvatting van het beveiligingsincident, wat is er met de gegevens gebeurd, wat voor gegevens zijn het (bijzondere gegevens of van gevoelige aard)
- Datum/periode van het beveiligingsincident

5.3. Beoordelen

Wanneer het Meldpunt voldoende informatie heeft verzameld en een datalek vermoedt, stuurt deze de FG een verzoek om de verzamelde informatie te bekijken. De FG beoordeelt de feiten om te bepalen of een melding aan de Autoriteit persoonsgegevens en/of betrokkene(n) vereist is.
Bij de beoordeling of er sprake is van een 'meldingsplichtig datalek', houdt de melder rekening met het type gegevens en de hoeveelheid gegevens. 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 moet het gemeld worden bij de Autoriteit Persoonsgegevens.
Er is sprake van ernstige nadelige gevolgen of de kans op ernstige nadelige gevolgen als er bijvoorbeeld heel veel gegevens van één of enkele betrokkene(n) of enkele gegevens van heel veel betrokkenen gelekt zijn. Ook wanneer de gelekte gegevens "gevoelig" zijn, zoals bijvoorbeeld bijzondere persoonsgegevens over gezondheid, over de financiële of economische situatie van de betrokkene, of als de gegevens kunnen leiden tot stigmatisering van de betrokkene, zijn er ernstige nadelige gevolgen.
Als sprake is van een datalek, dan legt de Ontdekker (medewerker) de volgende informatie in het formulier van datalekken vast:

- Omschrijving (wat is er precies gebeurd)
- Datum/tijd van het datalek (indien mogelijk)
- Duur van de inbreuk (hoe lang heeft het geduurd voordat een einde is gemaakt aan de inbreuk)
- Datum/tijd ontdekking van het datalek
- Datum/tijd melding van het datalek
- Categorie persoonsgegevens
- Categorie doelgroep
- Lekhoeveelheid
- Betrokkenen
- Maatregelen

Indien de Ontdekker een inwoner is, legt de PO de hiervoor benoemde informatie in het formulier van datalekken vast.

5.4. Repareren

Indien van toepassing, achterhaalt de Technicus de oorzaak van het beveiligingsincident en/of datalek en laat de oorzaak verhelpen. De Technicus legt vast:

- Technische maatregelen die genomen zijn om de inbreuk te verhelpen en verdere inbreuk te voorkomen (voor zover de oorzaak bekend is).
- Of de gelekte gegevens onbegrijpelijk zijn voor degenen die er kennis van hebben kunnen nemen? Of de gegevens onbegrijpelijk zijn gemaakt (versleuteld)?

5.5. Melden

Wanneer er sprake is van een ernstig datalek of wanneer niet duidelijk is of er sprake is van een ernstig datalek overlegt de FG met de directeuren van HLTsamen. Als de conclusie is dat er als dan niet voorlopig een melding gedaan moet worden bij de Autoriteit Persoonsgegevens (en eventueel betrokkenen), dan doet de PO dit binnen 72 uur namens de organisatie. Een voorlopige melding kan altijd ingetrokken worden. Het lek wordt gemeld bij het meldloket datalekken van de Autoriteit Persoonsgegevens.

5.6. Vastleggen

Alle informatie, die in de stappen 1 t/m 5 is ingewonnen of ontstaan, wordt gearchiveerd door het Meldpunt. Hiermee is het incident afgesloten. Alle (ernstige) datalekken worden door de PO vastgelegd in een apart register. Het Meldpunt stuurt een samenvatting van de genomen maatregelen aan de Ontdekker en bespreekt met de teammanager van het betreffende team welke maatregelen getroffen kunnen worden om het incident of datalek in de toekomst te voorkomen.

5.7. Informeren betrokkenen

Heeft het datalek mogelijk ongunstige gevolgen voor de persoonlijke levenssfeer van de betrokkene(n)? Dan meldt het vakteam waar het datalek ontstaan is, het datalek ook aan de betrokkene(n) zelf. Denk hierbij aan medewerkers, inwoners of ouders van inwoners als zij jonger zijn dan 16 jaar. Het vakteam verstuurt de brief na afstemming met de FG en team Communicatie.
Let op: zijn de gelekte persoonsgegevens beveiligd of versleuteld en is de gelekte data onbegrijpelijk of ontoegankelijk voor anderen? Dan hoeft dat niet aan de betrokkene(n) te worden gemeld.