Protocol informatiebeveiligingsincidenten en datalekken

Datum	Omschrijving
23-1-2019	Vastgesteld door Directie en stuurgroep IBP
13-2-2019	Instemming GMR

Vastgesteld door Stichting Openbaar Voortgezet Onderwijs Tilburg (SOVOT)

Datum	Naam	Functie
14-2-2019	N.F.J. Bootsma	Bestuurder

Inhoud

Inleiding

Dit protocol biedt een handleiding voor een correcte afhandeling van beveiligingsincidenten en datalekken. In dit protocol wordt omschreven hoe Sovot omgaat met het beoordelen en zo nodig melden van beveiligingsincidenten en datalekken. Dit protocol sluit aan bij het Informatiebeveiligings- en privacybeleid van Sovot.

Gebruikte termen:

- **Beveiligingsincident**; een beveiligingsincident is een gebeurtenis die er voor zorgt of zou kunnen zorgen dat de beschikbaarheid, integriteit en/of vertrouwelijkheid van de informatievoorziening wordt aangetast.
- **Informatievoorziening**; het geheel van mensen, middelen en maatregelen, gericht op de informatiebehoefte van de organisatie.
- **Datalek**; een beveiligingsincident waarbij persoonsgegevens verloren raken of onrechtmatig worden bewerkt (opgeslagen, aangepast, verzonden, et cetera). Alle datalekken zijn beveiligingsincidenten, maar niet alle beveiligingsincidenten zijn datalekken.
- **Betrokkene**; de persoon van wie de persoonsgegevens zijn gelekt.

Wet- en regelgeving datalekken

Op 1 januari 2016 is de meldplicht datalekken toegevoegd aan de Wet bescherming persoonsgegevens (Wbp). Door deze meldplicht zijn scholen en schoolbesturen verplicht melding te maken van ernstige datalekken bij de Autoriteit Persoonsgegevens. Sinds 25 mei 2018 is de Algemene Verordening Gegevensbescherming (AVG) van kracht. De meldplicht datalekken blijft daarmee gelden. De eisen voor registratie zijn wel strenger geworden en boetes bij overtreding hoger.

De meldplicht is alleen van toepassing wanneer het persoonsgegevens betreft. Dit heeft bijvoorbeeld betrekking op persoonsgegevens uit de leerlingen- en personeelsadministratie. Er is sprake van een datalek wanneer er bij een beveiligingsincident persoonsgegevens verloren zijn gegaan, of wanneer het niet valt uit te sluiten dat persoonsgegevens verloren zijn gegaan of in handen van onbevoegden zijn terecht gekomen.

De meldplicht bij een datalek geldt voor de verantwoordelijke voor de persoonsgegevens. Dat is het bestuur van Sovot. Het bestuur zal zich laten bijstaan door de Functionaris Gegevensbescherming in de overweging of een incident gemeld moet worden en waar nodig bij de beantwoording van de vragen. De melding gebeurt eveneens in samenwerking met de medewerker die belast is met het Meldpunt Datalekken.

Wanneer er een datalek wordt geconstateerd waarvan melding moet worden gemaakt, moet dat binnen 72 uur na ontdekking van het lek worden gemeld bij de Autoriteit Persoonsgegevens, ook als nog niet alle informatie voorhanden is en de melding nog niet volledig gedaan kan worden.

Afspraken met externe partijen

Sovot maakt gebruik van diensten van derden, zoals softwareleveranciers. Wanneer zij persoonsgegevens namens Sovot verwerken, sluit Sovot met hen een verwerkersovereenkomst af. Daarin worden aanvullende afspraken gemaakt omtrent het verwerken van persoonsgegevens en het voorkomen en afhandelen van beveiligingsincidenten. Ook zijn er partijen waaraan Sovot persoonsgegevens beschikbaar stelt in het belang van het onderwijs of van betrokkenen, zoals de openbare bibliotheek. Ook met die partijen is een verwerkersovereenkomst afgesloten.

In de verwerkersovereenkomst zijn in ieder geval afspraken omtrent de volgende punten opgenomen:

- Hoe informeren partijen elkaar bij een beveiligingsincident of een mogelijk datalek?

- Wie doet melding bij de Autoriteit Persoonsgegevens en indien nodig bij de betrokkenen?
- Welke informatie wordt door de verwerker met Sovot gedeeld bij een datalek?
- Welke informatie is nodig voor het maken van een melding?

Werkwijze

Er zijn vijf rollen die van belang zijn bij het afhandelen van een beveiligingsincident.

1. **Ontdekker**; degene die het beveiligingsincident of datalek op het spoor komt en het proces in werking stelt.
2. **Meldpunt datalekken**; de medewerker van Sovot die alle beveiligingsincidenten registreert en verwerkt. Bereikbaar via datalek@sovot.nl.
3. **Melder**; degene die verantwoordelijk is voor het melden van een datalek bij de Autoriteit Persoonsgegevens. Dit zijn de medewerker, die belast is met het Meldpunt datalekken, en de bestuurder.
4. **Technicus;** degene die de oorzaak van het datalek kan vinden en kan (laten) repareren.
5. **Functionaris voor de gegevensbescherming**; adviseur voor SOVOT voor de bescherming van persoonsgegevens.

Er zijn zeven stappen die doorlopen worden bij een beveiligingsincident.

1. **Ontdekken**
   De Ontdekker merkt een beveiligingsincident op, via eigen waarneming of via waarneming van een derde. De Ontdekker verzamelt zoveel mogelijk informatie over het beveiligingsincident en meldt het bij het meldpunt datalekken via datalek@sovot.nl.

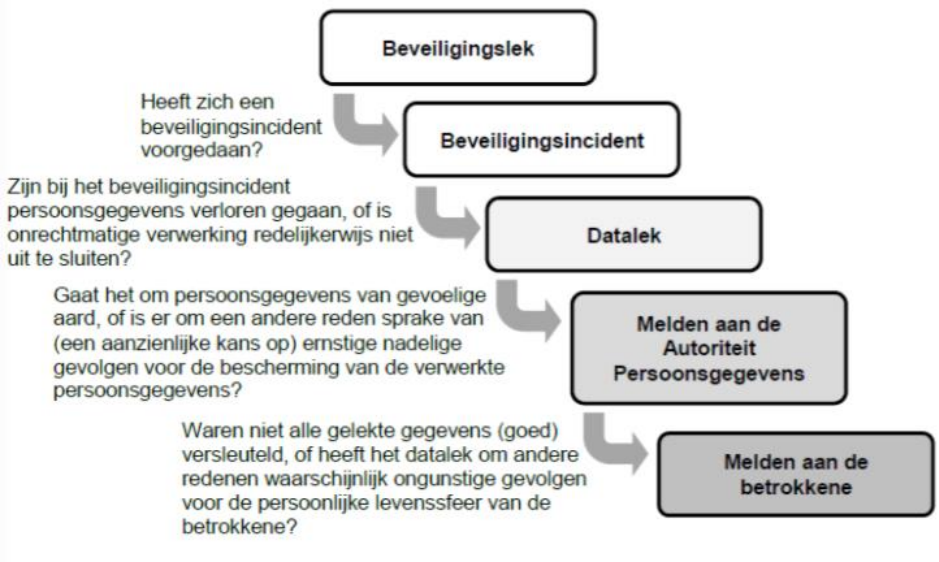
2. **Inventariseren**
   Het meldpunt datalekken bepaalt dan of er voldoende informatie omtrent het beveiligingsincident bekend is. Zo niet, dan zet hij/zij aanvullende vragen uit bij de Ontdekker en/of de Technicus. De volgende informatie wordt daarna vastgelegd door het meldpunt datalekken:
   - Datum/periode van het beveiligingsincident
   - Aard van het beveiligingsincident
   - Wanneer van toepassing (bij een datalek):
     - Omschrijving van de groep betrokkenen
     - Aantal betrokkenen
     - Type persoonsgegevens in kwestie
     - Worden de gegevens binnen een keten gedeeld
   - Samenvatting van het beveiligingsincident; wat is er met de gegevens gebeurd, welk type gegevens betreft het (bijzondere persoonsgegevens of van gevoelige aard), et cetera.

3. **Beoordelen**
   Wanneer het Meldpunt datalekken voldoende informatie heeft verzameld en een datalek vermoedt, stuurt deze de Melder een verzoek om de verzamelde informatie te beoordelen. De Melder/bestuurder beoordeelt de feiten om te bepalen of een melding aan de Autoriteit Persoonsgegevens en/of betrokkenen vereist is.
   De volgende informatie wordt in het incidentenregister vastgelegd door de Melder:
   - Mogelijke gevolgen voor de persoonlijke levenssfeer van de betrokkenen.
   - Wordt het datalek gemeld aan de Autoriteit Persoonsgegevens? Waarom wel/niet?
   - Wordt het datalek aan betrokkenen gemeld? Waarom wel/niet?
   - Wat is de inhoud van de melding?

   Bij de beoordeling of er sprake is van een meldingsplichtig datalek wordt rekening gehouden met het type gegevens en de hoeveelheid gegevens. Het datalek dient gemeld te worden aan de Autoriteit Persoonsgegevens tenzij het niet waarschijnlijk is dat het datalek een risico inhoudt voor de rechten

en vrijheden van de betrokkene(n), zulks ter finale beoordeling aan de bestuurder. Indien het datalek leidt tot ernstige nadelige gevolgen voor de bescherming van persoonsgegevens van betrokkenen, of een aanzienlijke kans daarop, moet er gemeld worden. Dit kan bijvoorbeeld het geval zijn wanneer de gelekte gegevens gevoelig zijn, zoals bijzondere persoonsgegevens inzake gezondheid, financiële of economische situatie van de betrokkene, of wanneer de gegevens kunnen leiden tot stigmatisering van de betrokkene.

De onderstaande beslisboom geeft de beoordeling van een beveiligingsincident weer.



4. Repareren

De Technicus wordt gevraagd te achterhalen wat de oorzaak van het beveiligingsincident is en moet de oorzaak (laten) verhelpen. De technicus van Sovot legt onderstaande vast:

- Technische en organisatorische maatregelen die genomen zijn om het beveiligingsincident te verhelpen en verdere incidenten te voorkomen. Dit voor zover de oorzaak bekend is.
- Zijn de gelekte gegevens onbegrijpelijk voor degenen die er kennis van heeft kunnen nemen? Hoe zijn de gegevens versleuteld?

5. Melden

Indien de conclusie bij stap 3 is dat er melding gedaan moet worden bij de Autoriteit Persoonsgegevens (en eventueel betrokkenen), dan zal de Melder dit binnen 72 uur na ontdekking doen via de link https://datalekken.autoriteitpersoonsgegevens.nl/melding/aanmaken. De melding bevat alle verzamelde informatie en de getroffen incidentele en structurele technische en organisatorische maatregelen.

6. Vastleggen

Alle informatie die in de voorafgaande stappen is ingewonnen of ontstaan, wordt in het incidentenregister gearchiveerd door het Meldpunt datalekken. Het Meldpunt datalekken verstuurt een samenvatting van de genomen maatregelen aan de Ontdekker.

7. Informeren betrokkenen

Als het datalek waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van betrokkene(n) stelt SOVOT onverwijld de betrokkene(n) daarvan in kennis. De tekst voor dit bericht dient door de

bestuurder opgesteld, dan wel goedgekeurd te worden alvorens verzending plaatsvindt. De bestuurder kan zich hierbij laten adviseren door de Functionaris voor Gegevensbescherming. Betrokkenen kunnen medewerkers, leerlingen (of hun ouders wanneer zij jonger zijn dan 16 jaar), ouders of andere belanghebbenden zijn.

Bij zeer ernstige datalekken met een groot risico voor (reputatie-)schade voor SOVOT overweegt de bestuurder tevens om stakeholders zoals personeel, gemeente en leveranciers te informeren over het datalek en de genomen maatregelen.

Monitoring beveiligingsincidenten en datalekken

Het Meldpunt datalekken van Sovot maakt jaarlijks aan de hand van het incidentenregister een analyse van de meldingen van beveiligingsincidenten en datalekken in samenwerking met de Functionaris Gegevensbescherming.

In deze analyse wordt ingegaan op eventuele structurele ontwikkelingen, en de noodzaak om maatregelen te nemen om herhaling te voorkomen. Het bestuur van Sovot wordt geïnformeerd over de uitkomsten van deze analyse en de voorstellen ter verbetering en voorkoming.