Protocol privacyincidenten en datalekken

Jan Tinbergen College
Vastgesteld: mei 2018
Aangepast: maart 2021

1. Inleiding

Het Protocol privacy-incidenten en datalekken sluit aan bij de uitgangspunten in het informatiebeveiligings- en privacy beleid (IBP) van het SOVOR en geldt voor het Jan Tinbergencollege (JTC).
Dit protocol biedt een handleiding voor de professionele melding, beoordeling en afhandeling van privacyincidenten en datalekken. Het doel hiervan is het voorkomen van privacyincidenten en datalekken.

Dit protocol is van toepassing op de gehele organisatie van het JTC en al haar medewerkers.

Gebruikte termen:

- **Privacyincident**; dit is een gebeurtenis waarbij de privacy van een medewerker, leerling of ouder binnen het JTC in het geding is of zou kunnen zijn. Hieronder verstaan we ook zaken die zouden kunnen zorgen of zorgen dat de beschikbaarheid, integriteit en/of vertrouwelijkheid van de persoonsgegevens worden aangetast.
- **Informatievoorziening**; het geheel van mensen, middelen en maatregelen, gericht op de informatiebehoefte van de organisatie.
- **Datalek**; een privacyincident waarbij persoonsgegevens verloren raken of onrechtmatig worden bewerkt (opgeslagen, aangepast, verzonden, et cetera). Alle datalekken zijn privacy-incidenten, maar niet alle privacyincidenten zijn datalekken.
- **Betrokkene**; de persoon van wie de persoonsgegevens zijn gelekt of wiens privacy in het geding is. Hier vallen tevens de personen binnen die betrokken zijn bij de oorzaak van het incident.

2. Wet- en regelgeving datalekken

Het JTC is wettelijk verplicht melding te maken van ernstige datalekken bij de Autoriteit Persoonsgegevens. De meldplicht is alleen van toepassing wanneer persoonsgegevens worden verwerkt, bijvoorbeeld in de leerlingenadministratie of digitale leermiddelen. Het JTC maakt met leveranciers die persoonsgegevens ontvangen aanvullende afspraken over het melden van datalekken.

Er is sprake van een datalek als er bij een privacyincident persoonsgegevens verloren zijn gegaan óf indien het niet valt uit te sluiten is dat persoonsgegevens verloren zijn gegaan. Er is persoonlijke informatie ‘gelekt’. Voorbeelden zijn een hack waarbij een database met persoonsgegevens is gestolen, het verliezen van een usb-stick met daarop de adresgegevens van een klas, het in de trein achterlaten van een dossier waarin van een leerling rapportages zijn opgenomen..

De meldplicht geldt voor de verantwoordelijke voor de persoonsgegevens, dat is dus het schoolbestuur. Een leverancier is een verwerker voor de school. Er kan met verwerkers worden afgesproken dat zij **namens** de verantwoordelijke de melding doet, maar dat gebeurt dan onder verantwoordelijkheid van het schoolbestuur.

Als er een datalek is, moet daar binnen 72 uur na ontdekking van het lek melding van worden gedaan bij de Autoriteit Persoonsgegevens.

3. Afspraken met leveranciers

Het schoolbestuur heeft verwerkingsovereenkomsten met alle leveranciers die persoonsgegevens ontvangen. Afspraken over datalekken vallen daar ook onder. Afspraken gaan o.a. over:

- Hoe informeer je elkaar over datalekken, en zorg ook voor bereikbaarheid tijdens bijvoorbeeld het weekend en vakanties.
- Wie doet de melding bij de Autoriteit Persoonsgegevens.
- Welke informatie de bewerker moet geven bij een datalek.
- Welke informatie nodig is voor het doen van een melding, en dat je elkaar informeert over de melding (maak afspraken dat je een kopie van de melding krijgt of doorstuurt).
- De tijd waarbinnen de bewerkers de gegevens moet aanleveren.
- Wie de communicatie met de gebruikers voor haar rekening neemt als dat nodig is.

De afspraken met uw verwerkers zijn vastgelegd in verwerkingsovereenkomsten, gebaseerd op het meest recente convenant “Digitale onderwijsmiddelen en privacy”.

4. Werkwijze

Uitgangssituatie

Uitgangspunt voor dit protocol is:

- Het document IBP (informatiebeveiligings- en privacy beleid) van het JTC;
- Het aanvaardbaar gebruik van bedrijfsmiddelen, waaronder de gedragscode voor ict en internetgebruik.
- De benodigde rollen voor de uitvoering zijn adequaat ingevuld: de privacy officer en de Functionaris Gegevensbescherming.

De zes rollen

Er zijn zes rollen die onderscheiden moeten worden om een privacy-incident en/of datalek succesvol af te handelen:

1. **Ontdekker**; degene die het privacy-incident of datalek op het spoor komt en het proces in werking stelt. Dit kan elke medewerker zijn.
2. **Meldpunt**; een centrale locatie waar alle privacy-incidenten of datalekken worden geregistreerd en verder worden verwerkt. Hiertoe is een meldfunctionaliteit ingericht welke via de site, en het intranet bereikbaar is. Incidenten worden automatisch geregistreerd binnen de YourSafetyNet omgeving (YSN) van het JTC, ze worden daarbij direct opgeslagen in het datalek/privacy-incident register. Meldingen worden automatisch doorgegeven aan de privacy officer (PO) die als analist incidenten fungeert.
3. **De veroorzaker** de persoon of personen wiens handelingen het incident veroorzaakt hebben.
4. **Melder**; degene die verantwoordelijk is voor het melden van een datalek bij de Autoriteit Persoonsgegevens. Voor het JTC is dit de Functionaris Gegevenbescherming (FG).
5. **Afdeling ICT**; in het geval dat een met ICT-gebruik gerelateerd datalek of privacy-incident aan de orde is en de oorzaak van het incident gevonden moet worden en gerepareerd kan worden. Voor het JTC is dit de systeembeheerder en/of applicatiebeheerder onder verantwoordelijkheid van de Portefeuillehouder ICT.
6. **Het bestuur**, de eindverantwoordelijke voor het privacybeleid van het Jan Tinbergen College.
7. **Het IRT**, incident response team, bestaande uit de FG, PO (evt. met assistent) en het bestuur.

N.B. Binnen het incidenten registratiesysteem van YourSafetyNet spelen de met groen aangegeven riollen een cruciale rol.

De zeven stappen

Deze stappen kunnen vanaf stap 2 simultaan plaatsvinden

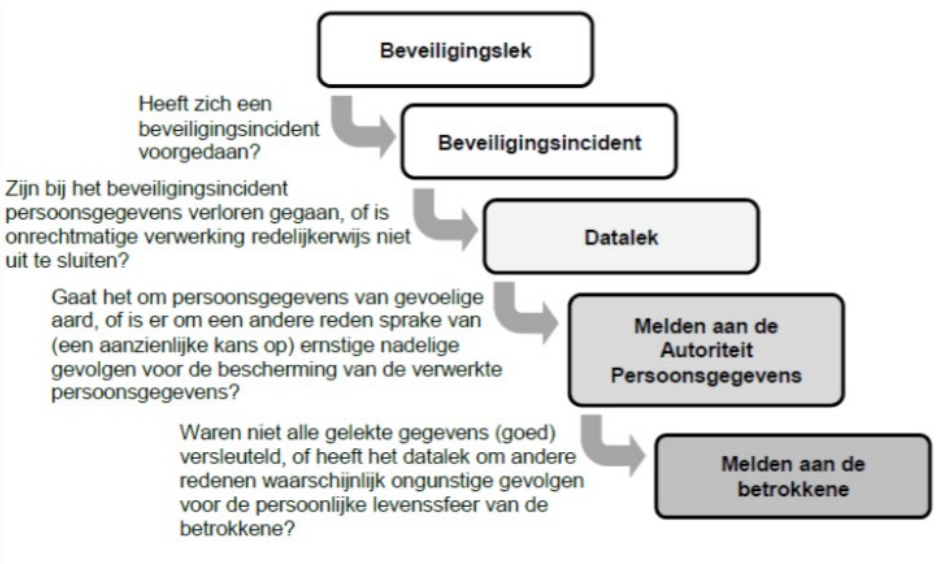
1. **Ontdekken**
   De Ontdekker merkt een privacyincident op. Via eigen waarneming of via waarneming van een derde. De Ontdekker verzamelt zoveel mogelijk informatie over het privacyincident en meldt het bij het meldpunt op sharepoint of de site. Het is ook mogelijk om direct te melden bij de privacy officer

2. **Inventariseren/analyseren**
   De privacy officer bepaalt of er voldoende informatie omtrent het privacyincident bekend is. Zo niet, dan zet hij aanvullende vragen uit bij de Ontdekker en/of deskundige en/of andere functionarissen. De volgende informatie wordt daarna vastgelegd:
   - Samenvatting van het privacy-incident, wat is er met de gegevens gebeurd, wat voor gegevens zijn het (bijzondere gegevens of van gevoelige aard)
   - Datum/periode van het privacy-incident
   - Aard van het privacy-incident
   - Wanneer van toepassing :
     - Omschrijving van de groep betrokkenen
     - Aantal betrokkenen
     - Type persoonsgegevens in kwestie
     - Worden de gegevens binnen een keten gedeeld

3. **Beoordelen**
   Wanneer de PO voldoende informatie heeft verzameld en vermoedt dat er inderdaad sprake is van een datalek, stuurt deze, via de YSN-omgeving, de FG een verzoek om de verzamelde informatie te bekijken. Tevens wordt het bestuur geïnformeerd.
   De FG beoordeelt de feiten om te bepalen of een melding aan de Autoriteit persoonsgegevens en/of betrokkenen vereist is.
   De volgende informatie wordt vastgelegd door de FG:
   - Mogelijke gevolgen voor de persoonlijke levenssfeer van de betrokkenen
   - Wordt het datalek gemeld aan de Autoriteit Persoonsgegevens? Waarom niet?
   - Wordt het datalek aan betrokkenen gemeld? Waarom niet?
   - Hoe worden meldingen gedaan? Wat is de inhoud van de melding?

   Bij de beoordeling of er sprake is van een ‘meldingsplichtig datalek’, hou je rekening met het type gegevens, en met de hoeveelheid gegevens. Indien het datalek leidt tot
   a. een aanzienlijke kans op ernstige nadelige gevolgen voor de bescherming van persoonsgegevens, of
   b. als het ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens,
   dan moet er gemeld worden.
   Van die ernstige nadelige gevolgen of de kans op ernstige nadelige gevolgen is bijvoorbeeld sprake wanneer er heel veel gegevens van een betrokkene of gegevens van heel veel betrokkenen gelekt zijn maar 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 (denk aan het lekken van een leerling die vaak kinderen pest en daarmee gezien kan worden als notoire pester).

De onderstaande beslisboom kan gebruikt worden



De FG betrekt bij het beoordelen het IRT (incident response team). Uiteindelijk besluit het bestuur of er een melding bij de AP gedaan wordt.

4. Repareren

Er wordt onderzocht of het incident tot gevolg heeft dat er iets gerepareerd moet worden, dit kan zijn in de zin van procedure, in de zin van ICT of vanuit het oogpunt van privacy by design of default.
Er wordt nagegaan wat de oorzaak van het privacyincident is en indien mogelijk wordt de oorzaak verholpen.
Het volgende wordt vastgelegd:

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

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 FG dit binnen twee werkdagen doen. De melding bevat alle verzamelde informatie en de getroffen incidentele en structurele technische en organisatorische maatregelen. Het lek wordt gemeld bij het meldloket datalekken: https://datalekken.autoriteitpersoonsgegevens.nl/actionpage?0.

6. Vastleggen

Alle informatie, die in de voorafgaande stappen is ingewonnen of ontstaan, wordt gearchiveerd door de PO waarmee het incident is afgesloten. Hiervoor wordt gebruik gemaakt van het register in de YSN-omgeving van de school. Indien mogelijk wordt in het kader van bewustwording het incident geanonimiseerd gepubliceerd binnen de school.

7. **Informeren betrokkenen: medewerkers, leerlingen en/of zijn ouders**
   Heeft het incident waarschijnlijk ongunstige gevolgen voor de persoonlijke levenssfeer van de betrokkene? Dan wordt het incident aan de betrokkenen gemeld. Dat zijn medewerkers, leerlingen (of hun ouders als zij jonger zijn dan 16 jaar) en ouders. In principe kan er van worden uitgaan dat het lekken van gevoelige aard gelekt gemeld moet worden bij de betrokkenen.
   Let op: als er persoonsgegevens zijn gelekt maar die zijn beveiligd of versleuteld, en de gelekte data zijn onbegrijpelijk of ontoegankelijk voor anderen, dan hoeft dat niet aan betrokkenen te worden gemeld. Denk aan het lekken van een beveiligde én versleutelde database met gebruikersnamen en wachtwoorden.

8. Monitoring en communicatie

Het Meldpunt van SOVOR maakt minimaal eenmaal per jaar een analyse van de meldingen van privacyincidenten en datalekken in samenwerking met de functionaris gegevensbescherming. In de analyse wordt ingegaan op eventuele structurele ontwikkelingen, en of de noodzaak bestaat om maatregelen te nemen om herhaling te voorkomen. Het bestuur wordt geïnformeerd over de uitkomsten van de analyse.

Datalekken worden (geanonimiseerd) in de interne communicatie gebruikt om het belang van data-veiligheid en de kwetsbaarheid van interne processen te onderstrepen.

Bij datalekken met (potentieel) gevolgen voor imago-schade of consequenties die de interne situatie van de school overstijgen, treedt het crisisprotocol van het JTC in werking. De directie bepaalt op welk moment en hoe er extern wordt gecommuniceerd.