
Procedure datalekken

6 september 2024

Versie 0.2

Inhoud

1. Inleiding	3
1.1. Definities	3
2. Datalekken bij het fonds	3
2.1. Interne datalekproces	3
3. Datalekken bij uitbestedingsrelaties	4
3.1. Externe datalekproces	4
4. Procedure melding aan AP of betrokkenen	4
4.1. Wanneer is er sprake van een Datalek?	4
4.2. Wanneer moet een Datalek worden gemeld aan de AP?	4
4.3. Inhoud melding	5
4.4. Inhoud melding aan Betrokkene(n)	5
4.5. Termijn melding aan AP	5

Document management

Datum	Veranderingen	Auteur(s)	Review	Versie
27 juni 2024	Draft	Stefan van de Giessen Thalis Cabral		0.1
6 sept. 2024	Aanpassing artikel 2, lid N	Commissie Uitbesteding, Uitvoering & Communicatie		0.2

1. Inleiding

Iedereen heeft recht op eerbiediging en bescherming van zijn persoonlijke levenssfeer en een zorgvuldige omgang met zijn persoonsgegevens. De regels hiervoor zijn vastgelegd in de Wet Algemene Verordening Gegevensbescherming (AVG).

Stichting Pensioenfonds Capgemini (hierna: SFPC, of 'het fonds') hecht grote waarde aan de (bescherming van de) privacy rechten van haar deelnemers, pensioen- en andere aanspraakgerechtigden en aan adequate beveiliging van haar data en heeft hier dan ook passende organisatorische maatregelen voor getroffen. Toch kan het voorkomen dat er een datalek optreedt binnen SPFC of bij één van haar uitbestedingsrelaties.

1.1. Definities

In deze Procedure datalekken worden de volgende begrippendefinities gehanteerd:

- **Betrokkene:** de persoon van wie de Persoonsgegevens zijn gelekt.
- **Datalek:** een inbreuk op de beveiliging van persoonsgegevens;
- **Inbreuk:** 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;
- **Meldplicht:** indien de Inbreuk een risico inhoudt voor de rechten en vrijheden van de Betrokkene, geldt de wettelijke plicht om de Inbreuk of een vermoeden hiervan binnen 72 uur na ontdekking te melden bij de Autoriteit Persoonsgegevens (AP). Indien de Inbreuk een hoog risico inhoudt voor de betreffende Betrokkene, dient deze Betrokkene tevens onverwijld op de hoogte te worden gesteld;
- **Persoonsgegevens:** elk gegeven betreffende een geïdentificeerde of naar een te identificeerbare persoon te herleiden gegeven zoals NAW gegevens, IP-adressen en foto's.

In deze procedure is uitgewerkt hoe er moet worden gehandeld als een (mogelijk) Datalek wordt geconstateerd door SPFC of wordt gemeld aan het fonds. Het bestuur van SPFC is verantwoordelijk voor de vaststelling van deze procedure, en de opvolging ervan.

2. Datalekken bij het fonds

2.1. Interne datalekproces

- a) De Privacy Officer is de aanspreekpunt voor datalekken.
- b) Als door de Privacy Officer een Datalek wordt geconstateerd of er een vermoeden is dat hiervan sprake is, wordt het Datalek gemeld bij de voorzitter van de Commissie Uitbesteding en Uitvoering (CUUC).
- c) De voorzitter van de CUUC informeert onverwijld het bestuur over het mogelijke Datalek.
- d) De Privacy Officer beoordeelt in samenspraak met de voorzitter van de CUUC of er daadwerkelijk sprake is van een Datalek en zo ja, of er sprake is van een Datalek waarvan melding gedaan moet worden bij de AP. Bij twijfel wordt er contact gezocht met de AP.
- e) Indien uit de beoordeling blijkt dat er sprake is van een Datalek dat gemeld moet worden, doet de Privacy Officer deze melding aan de AP zonder onredelijke vertraging en indien mogelijk, uiterlijk binnen 72 uur nadat hij kennis van het (mogelijke) Datalek heeft genomen. Indien de melding aan de AP niet binnen 72 uur plaatsvindt, gaat de melding vergezeld van een motivering voor de vertraging. Bij de melding wordt gebruik gemaakt van het webformulier van de AP.
(<https://datalekken.autoriteitpersoonsgegevens.nl/actionpage>).
- f) Indien en voor zover het niet mogelijk is om alle informatie gelijktijdig te verstrekken, kan de informatie zonder onredelijke vertraging in stappen worden verstrekt. Een melding van een Datalek kan achteraf worden ingetrokken als blijkt dat er geen Meldplicht bestond.
- g) Indien er sprake is van een Datalek, beoordeelt de Privacy Officer tevens in samenspraak met het de

voorzitter van de CUUC, of het Datalek ook aan de Betrokkene(n) moet worden gemeld.

- h) De Privacy Officer verstrekt de beoordeling aan het bestuur. De beoordeling wordt dan geaccordeerd door de CUUC.
- i) Indien uit de beoordeling volgt dat de Betrokkene(n) geïnformeerd moet/moeten worden, wordt/worden de Betrokkene(n) telefonisch en/of schriftelijk door de voorzitter van de CUUC geïnformeerd.
- j) De verplichting om de Betrokkene(n) te informeren kan ook door de AP worden opgelegd. SPFC zal gevolg hieraan geven.
- k) De Privacy Officer onderzoekt in samenspraak met de voorzitter van de CUUC en/of het bestuur of:
 - er maatregelen genomen moeten worden om de gevolgen van het Datalek (onafhankelijk of deze moest worden gemeld of niet) te beperken;
 - procedures aangepast moeten worden om nieuwe Datalekken te voorkomen.
- l) De voorzitter van de CUUC rapporteert het Datalek aan het bestuur in de eerstvolgende CUUC-vergadering en informeert het bestuur over de eventueel genomen/nog te nemen maatregelen ter voorkoming van Datalekken.
- m) De Privacy Officer documenteert alle datalekken opgenomen in een Datalekregister. Hierin staan in ieder geval de feiten en gegevens van het Datalek (oorzaak Datalek, soort gegevens die gelekt zijn, het moment van ontdekking van het Datalek, op welke wijze het Datalek gedicht is, de melding aan de Betrokkene(n) e.d.).
- n) De Privacy Officer bewaart de gegevens, zoals vermeld in het voorgaande lid, minimaal één jaar. Indien het fonds heeft besloten, om zwaarwegende redenen, het datalek niet aan de betrokkene te melden, worden de gegevens minimaal drie jaar bewaard. In dit geval vindt er jaarlijks een evaluatie plaats om te bepalen of het datalek alsnog aan de betrokkene(n) moet worden gemeld.

3. Datalekken bij uitbestedingsrelaties

3.1. Externe datalekproces

Een datalek kan zich ook voordoen bij een partij aan wie het fonds werkzaamheden heeft uitbesteed. Het fonds heeft schriftelijke afspraken gemaakt met de uitbestedingsrelaties over hoe om te gaan met datalekken. Het fonds heeft vastgesteld dat de uitbestedingspartijen procedures hebben opgesteld, zodat het fonds kan voldoen aan de wet- en regelgeving op het gebied van datalekken.

Uitgangspunt is dat SPFC verantwoordelijk is voor het melden van datalekken. Indien een melding plaatsvindt aan het fonds door een uitbestedingspartij, wordt de procedure datalekken gevolgd.

4. Procedure melding aan AP of betrokkenen

4.1. Wanneer is er sprake van een Datalek?

Er is sprake van een Datalek als er een inbreuk op de beveiliging heeft plaatsgevonden 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.

Voorbeelden van Datalekken zijn: een kwijtgeraakte laptop/USB-stick met Persoonsgegevens, een inbraak in een databestand door een hacker, of het versturen van een pensioenopgave naar een andere deelnemer dan voor wie de opgave bedoeld is.

4.2. Wanneer moet een Datalek worden gemeld aan de AP?

Een Datalek moet worden gemeld aan de AP indien het Datalek een risico inhoudt voor de rechten en vrijheden van de Betrokkene(n).

Hiervan is sprake als:

- er persoonsgegevens zijn gelekt van gevoelige aard (waaronder gegevens over de financiële of economische situatie van Betrokkene, gegevens die kunnen leiden tot stigmatisering of uitsluiting van de Betrokkene, gebruikersnamen, wachtwoorden, gegevens die misbruikt kunnen worden voor (identiteits-)fraude);
- de aard en omvang van het Datalek tot (een aanzienlijke kans op) ernstige nadelige gevolgen leidt.

Hierbij is van belang:

- Gaat het om veel Persoonsgegevens per persoon of om gegevens van grote groepen?
- Zijn de beslissingen die op basis van de verwerkte Persoonsgegevens kunnen worden genomen ingrijpend?
- Worden de Persoonsgegevens binnen de verwerkingsketens gedeeld?
- Gaat het om Persoonsgegevens van kwetsbare groepen?

4.3. Inhoud melding

In de melding wordt ten minste het volgende omschreven of meegedeeld:

- de aard van de Inbreuk, waar mogelijk onder vermelding van de categorieën van Betrokkenen en persoonsgegevensregisters in kwestie en, bij benadering, het aantal Betrokkenen en persoonsgegevensregisters in kwestie;
- de naam en de contactgegevens van voorzitter van de CUUC of de Privacy Officer waar meer informatie kan worden verkregen;
- de waarschijnlijke gevolgen van de Inbreuk;
- de maatregelen die SPFC heeft voorgesteld of genomen om de Inbreuk aan te pakken, waaronder, in voorkomend geval, de maatregelen ter beperking van de eventuele nadelige gevolgen daarvan.

4.4. Inhoud melding aan Betrokkene(n)

In de kennisgeving aan de Betrokkene(n) moet in ieder geval in duidelijke en eenvoudige taal worden gemeld:

- de aard van het Datalek;
- de instanties waar de Betrokkene(n) meer informatie over het Datalek kan/kunnen krijgen;
- de waarschijnlijke gevolgen van het Datalek;
- de maatregelen die zijn aanbevolen of genomen om het Datalek aan te pakken, waaronder, in voorkomend geval, de maatregelen ter beperking van de eventuele nadelige gevolgen van het Datalek.

4.5. Termijn melding aan AP

Het Datalek moet zonder onredelijke vertraging, uiterlijk binnen 72 uur na ontdekking, worden gemeld aan de AP. De termijn voor het melden begint te lopen op het moment dat de verantwoordelijke of een verwerker op de hoogte raakt van een Datalek dat mogelijk onder de Meldplicht valt. De verantwoordelijke, mag na het ontdekken van het Datalek, enige tijd nemen voor nader onderzoek teneinde een onnodige melding te voorkomen. Wat in een concreet geval als 'zonder onredelijke vertraging' moet worden aangemerkt zal afhangen van de omstandigheden van het geval.

Vastgesteld op 6 september 2024 en laatstelijk vastgesteld door het bestuur op 6 september 2024.