Datalek procedure

Vastgesteld op	06-12-2023
Geldig tot	06-12-2025
Vastgesteld door	Directeur bedrijfsvoering Scala Sales & Consultancy

---

Aanleiding
Vanaf 1 januari 2016 is de meldplicht Datalekken van kracht. Dit houdt in dat bedrijven en organisaties die persoonsgegevens van klanten, medewerkers of ketenpartners verwerken, verplicht zijn om (potentiële) datalekken te melden aan de toezichthouder, de Autoriteit Persoonsgegevens. In bepaalde gevallen moet dit ook gemeld worden aan de betrokkene van wie de gegevens zijn gelekt. Als blijkt dat niet of onvoldoende is voldaan aan deze meldplicht kan de Autoriteit Persoonsgegevens een boete opleggen.

Wat is een datalek
Volgens de AVG is er sprake van een datalek als per ongeluk, opzettelijk of onrechtmatig persoonsgegevens vernietigd, verloren of gewijzigd worden, of als ongeautoriseerde openbaring van die gegevens plaatsvindt. Voorbeelden van een datalek zijn het verlies van een mobiel apparaat waarop gevoelige persoonsgegevens staan. Maar ook computer hacking, stroomuitval (waardoor gegevens verloren gaan) of inzage van privé gegevens door een onbevoegd persoon. Dit kan gebeuren doordat je bijvoorbeeld informatie per mail verstuurt aan een mailadres waarvan je niet zeker weet of dit ook bij de persoon in kwestie hoort. Ook als je gegevens over een betrokkene niet afschermt (bijvoorbeeld in een telefoongesprek) waardoor een ander persoon dingen hoort die herleidbaar zijn tot een privépersoon, dan is dat een datalek.

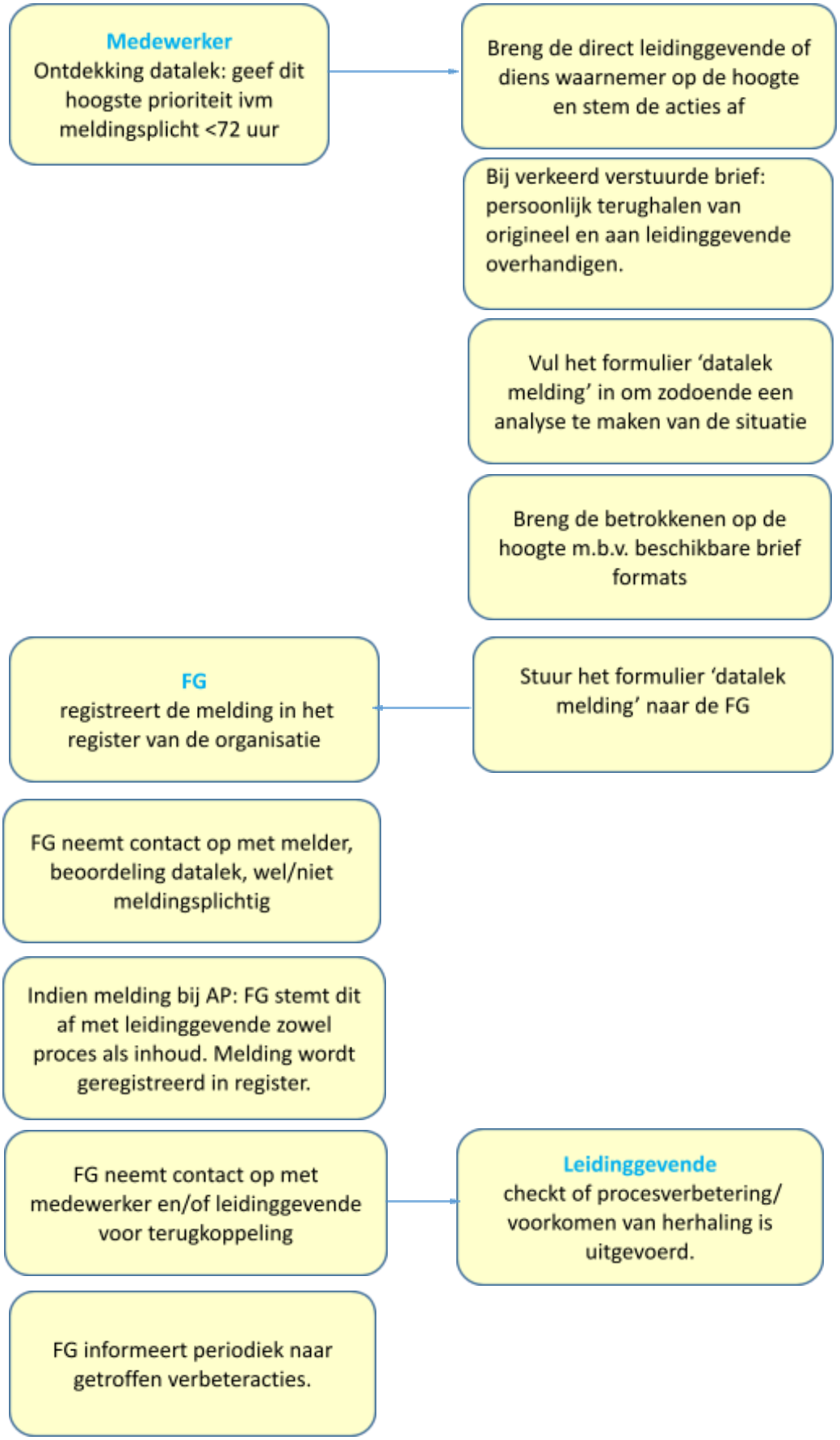
Melden bij de Autoriteit Persoonsgegevens
Niet ieder datalek-incident valt onder de meldplicht. Als bijvoorbeeld verloren of gestolen persoonsgegevens goed versleuteld zijn opgeslagen, dan is er geen aanzienlijk risico op schade aan de persoonlijke levenssfeer. Maar als bijvoorbeeld zonder toestemming van een betrokkene bekend wordt dat hij klant bij een bepaalde organisatie is, dan wordt dat als schadelijke inbreuk op de privacy beschouwd.

Een datalek dient uiterlijk *binnen 72 uur* na ontdekking te worden gemeld aan de toezichthouder. Deze melding wordt verzorgd door de Functionaris Gegevensbescherming (FG). Bovendien moet gemeld worden hoe het lek heeft kunnen plaatsvinden en wat er gedaan wordt om het lek te dichten. Het kan immers zijn dat een werkproces foutgevoelig is en voor verbetering vatbaar is. Daarom zal de FG bij een datalek altijd een analyse maken van de situatie en betrokkenen helpen met suggesties om herhaling te voorkomen.

Er moet in ieder geval gemeld worden als:

Zijn gegevens (definitief) verloren gegaan? Ja melden
Zijn de gegevens bijzonder of zeer omvangrijk? Ja melden
Zijn de gegevens in onbevoegde handen geraakt? Ja melden
Aanzienlijk risico op schade aan persoonlijke levenssfeer? Ja melden
Nee op alle vragen niet melden

Proces melden (vermoedelijk)datalek



Formulier datalek melding (versie 2024 Scala Arnhem)

1. Naam van de melder
2. Datum van het begin van het datalek
3. Bestaat het datalek nog voort? (datum einde datalek:)
4. Er is sprake van : ongeoorloofde vernietiging van persoonsgegevens/ ongeoorloofde wijziging van persoonsgegevens/ een onbevoegde heeft gegevens ingezien of kunnen inzien/ er is geen sprake van persoonsgegevens maar andere privacygevoelige gegevens, namelijk…….
5. Om gegevens van hoeveel betrokkenen gaat het? (één of meerdere personen en hoeveel dan)
6. Om hoeveel gegevens en welke gegevens gaat het? (voorbeelden: naam, geslacht, adres, geboortedatum, telefoonnummer, mailadres, BSN, medische gegevens, financiële gegevens, verzekeringsnummer, foto) Voeg zo mogelijk een kopie van het document toe.
7. Zijn de gegevens die gelekt zijn van een volwassene of van een kind (<18 jaar)?
8. Wie heeft het lek ontdekt? (is er een melder, bijvoorbeeld een andere cliënt, of is het door een collega ontdekt of door de melder)
9. Beschrijving van het incident
10. Wat is de mogelijke oorzaak van het incident?
11. Wat wordt er gedaan om herhaling te voorkomen?
12. Zijn de gelekte gegevens terug gehaald? Hoe is dit gebeurd?
13. Is de betrokkene van wie de gegevens gelekt zijn, ingelicht? Wat is er met die persoon gecommuniceerd (letterlijke weergave)?
14. Hoe reageerde de betrokkene (letterlijke weergave)?
15. Is de leidinggevende ingelicht?
16. Zijn er nog anderen betrokken zoals ketenpartners, medebehandelaars, softwareleverancier?
17. Op welk mobiel nummer kan de FG je bereiken (ook buiten kantooruren, dit ivm melding aan AP binnen 72 uur)?
18. Overige opmerkingen……..