Procedure datalekken

Dit document beschrijft de te doorlopen procedure bij het (vermoeden van) datalekken. Raadpleeg ook altijd de site van de Autoriteit Persoonsgegevens.

Een ieder kan deze procedure in gang zetten.

Eisen vanuit de AVG:

- Het melden aan de Autoriteit Persoonsgegevens (AP) is een zaak van de Verwerkingsverantwoordelijke.
  Vertaald naar ons is dat dus de klant wanneer het data van klanten betreft of wij zijn het zelf wanneer het onze eigen personele data betreft, in onze administraties vastgelegde contactgegevens van klanten zijn of persoonsgegevens die onder onze verantwoording door een andere partij worden verwerkt.

- Verantwoordelijke meldt waar mogelijk binnen 72 uur na bewustwording het datalek bij de AP.

- Er moet een register worden bijgehouden zodat de naleving gecontroleerd kan worden.

Procedure

1. Mogelijk datalek geconstateerd (is in feite nog geen onderdeel van de procedure)
2. Direct melden bij het bestuur (redstars@live.nl), bij voorkeur mondeling
3. Het bestuur registreert de melding, ongeacht het verdere verloop
4. Het bestuur maakt goede evaluatie van het risico
5. Het bestuur beoordeelt of melden bij AP noodzakelijk is (indien het gegevens zijn waar wij verantwoordelijk voor zijn)
6. Het bestuur beoordeelt of melden aan de Betrokkene noodzakelijk is (indien het gegevens zijn waar wij verantwoordelijk voor zijn
7. Het bestuur beoordeelt of melden bij Verantwoordelijke noodzakelijk is (indien het gegevens zijn waar de klant verantwoordelijk voor is)
8. Het bestuur beoordeelt of er vervolgacties nodig zijn (maatregelen ter voorkoming)
9. Het bestuur vult registratie aan met besluitvorming en genomen acties

Punt 4: Evaluatie van het risico

Om het risico in te kunnen schatten, zijn een aantal gegevens nodig. Mocht er een melding aan de AP gedaan moeten worden, dan moeten dezelfde gegevens opgevoerd worden.

Procedure datalekken

Van hoeveel personen zijn persoonsgegevens betrokken bij de inbreuk
- a: maximaal …
- b: minimaal …

Omschrijf de groep mensen van wie persoonsgegevens zijn betrokken bij de inbreuk

Wanneer vond de inbreuk plaats op/van-tot
- Op
- Van – tot

Wat is de aard van de inbreuk (meerdere opties mogelijk)
- lezen
- kopiëren
- veranderen
- verwijderen of vernietigen
- diefstal

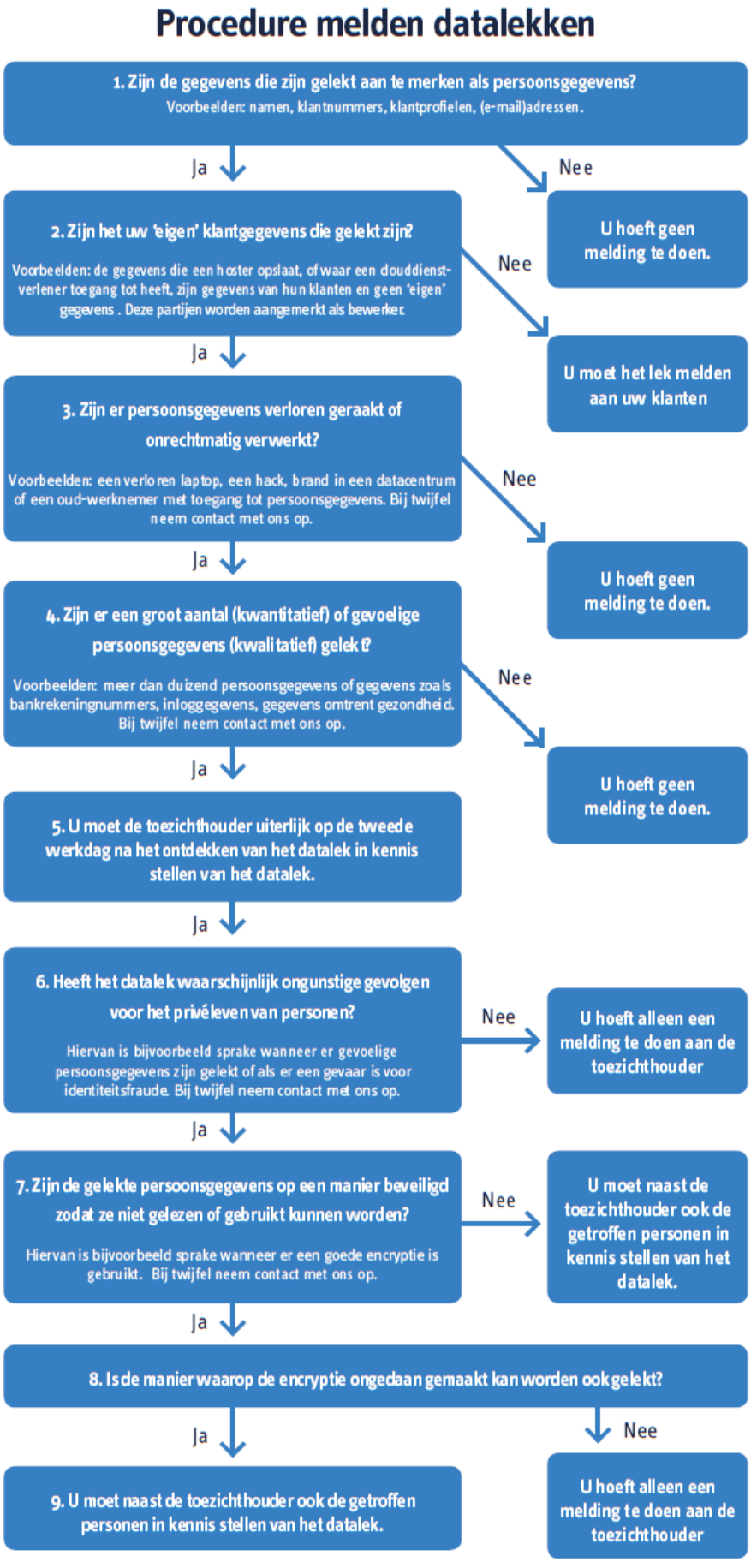
Om welk type persoonsgegevens gaat het (meerdere opties mogelijk)
- naam-,adres en woonplaats gegevens
- telefoonnummers
- e-mailadressen of andere adressen voor elektronische communicatie
- toegangs- of identificatiegegevens
- financiële gegevens
- bsn of sofinummer
- paspoort kopieën of kopieën van andere legitimatiebewijzen
- geslacht, geboortedatum en/of leeftijd
- bijzondere persoonsgegevens (b.v. ras, etniciteit, religie)
- overige gegevens, namelijk ….

Welke gevolgen kan de inbreuk hebben voor de persoonlijke levenssfeer van de betrokkenen (meerdere opties mogelijk)
- Stigmatisering of uitsluiting
- Schade aan de gezondheid
- Blootstelling aan (identiteits)fraude
- Blootstelling aan spam of phishing
- Anders, namelijk ….

Punt 5 Melden bij AP en Punt 6 Melden aan Betrokkenen

Gebruik het onderstaande schema om te bepalen of er een melding aan de toezichthouder gedaan moet worden en/of de getroffen personen in kennis gesteld moeten worden.

Procedure datalekken



Procedure datalekken

Melden bij AP?
Niet ieder datalek hoeft aan de AP gemeld te worden. Weeg het volgende af:
Is het onwaarschijnlijk dat de inbreuk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen? dan geen meldingsplicht. Wel registratieplicht uiteraard.
Anders verwoord: een inbreuk in verband met persoonsgegevens moet worden gemeld aan de toezichthouder, tenzij het lek geen risico oplevert op negatieve gevolgen als identiteitsfraude of reputatieschade.

Betrokkene informeren?
Melden bij de AP betekent niet dat ook de Betrokkene geïnformeerd moet worden. Weeg het volgende af:
Is het waarschijnlijk dat de inbreuk resulteert in een hoog risico voor zijn rechten en vrijheden zodat hij eventuele voorzorgsmaatregelen kan treffen? Zo nee, niet informeren.
Zo ja, zijn er maatregelen getroffen en toegepast op de betreffende persoonsgegevens? B.v. versleuteling zodat degene die de gegevens in handen krijgt niet kan achterhalen welke personen de gegevens betreffen of zijn er achteraf maatregelen genomen door de verantwoordelijke om te zorgen dat de hoge risico's voor de rechten en vrijheden van de betrokkene zich waarschijnlijk niet meer voor zullen doen.

De AVG schrijft voor wat er in de melding aan de AP omschreven moet worden. Informatie over de aard van de melding (eerste melding of vervolg op een eerdere melding), het wettelijk kader voor deze melding (Wbp of Tw), algemene informatie en contactgegevens, gegevens over het datalek, naar aanleiding van het datalek getroffen vervolgacties, informatie over het inlichten van patiënten, getroffen technische maatregelen, internationale aspecten en of er nog een vervolgmelding zal volgen.

Punt 9 Het register

Het register is bedoeld om te leren én om aan de AP aan te tonen dat datalekken daadwerkelijk gemonitord en opgevolgd worden.

Het register bevat:

- Een korte omschrijving van het lek
- Wanneer het plaats vond
- Wat er met de gegevens is gebeurd (zijn ze verloren gegaan, of door een onbevoegde ingezien, gekopieerd of gewijzigd)
- Van welke groep(en) personen er gegeven gelekt zijn, en om hoeveel personen het gaat.
- Om welke soort gegevens het gaat
- De (mogelijke) gevolgen van de inbreuk
- De maatregelen die genomen zijn naar aanleiding van het lek. Welke actie is ondernomen om de schade te voorkomen of zoveel mogelijk te beperken. En, wat is er gedaan om te zorgen dat het niet nog een keer zal gebeuren?