Protocol Meldplicht Data-lekken

1. Doel van het protocol

Het doel van de procedure meldplicht data-lekken is ervoor zorgdragen dat leden van, bezoekers aan of wedstrijddeelnemers van andere verenigingen bij Alliance d'Amitié in geval van een data-lek deze procedure volgen om de impact op de vereniging en andere belanghebbenden te minimaliseren.

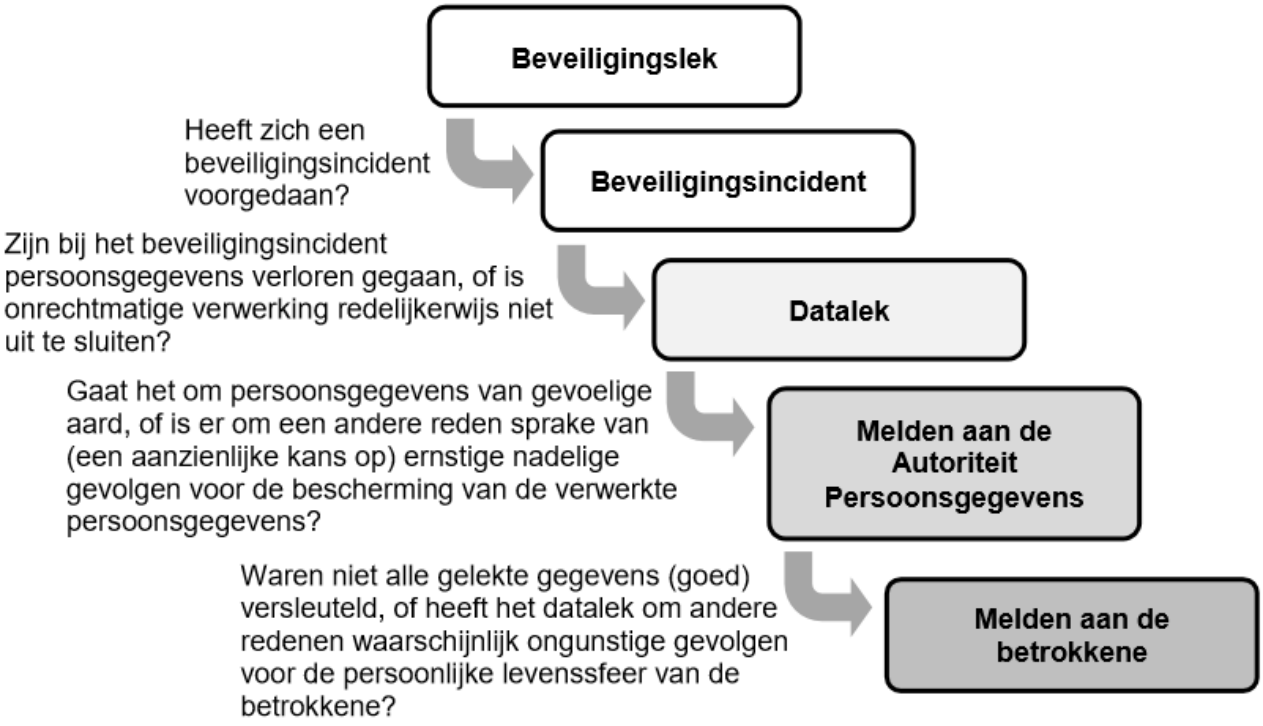
Er is geen sprake van verwerkers in de zin van de Algemene Verordening gegevensbescherming. Alliance d'Amitié is zelf gegevensverantwoordelijke.

2. Aanleiding voor het protocol

Sinds 1 januari 2016 geldt de meldplicht data-lekken. Deze meldplicht houdt in dat organisaties (zowel bedrijven als overheden) direct een melding moeten doen bij de Autoriteit Persoonsgegevens zodra zij een ernstig data-lek hebben. En soms moeten zij het data-lek ook melden aan de betrokkenen (de mensen van wie de persoonsgegevens zijn gelekt). De vestigingsplaats van de bewerker is voor de meldplicht data-lekken niet relevant. Ook data-lekken die plaatsvinden bij een buitenlandse bewerker (die gevestigd is in een andere EU-lidstaat of in een land buiten de EU) vallen onder dit protocol.

Afwegingen

Bij de beslissing of Alliance d'Amitié een gebeurtenis, die zich heeft voorgedaan, moet melden aan de Autoriteit Persoonsgegevens, en eventueel daarnaast ook aan de betrokkene, moet een aantal afwegingen gemaakt worden. Het onderstaande schema geeft deze afwegingen weer:



Figuur 1: uit Richtsnoeren Meldplicht data-lekken, autoriteit persoonsgegevens.

3. Wat zijn persoonsgegevens?

Een persoonsgegeven is "elk gegeven betreffende een geïdentificeerde of identificeerbare persoon".
Een persoon is identificeerbaar indien zijn identiteit redelijkerwijs, zonder onevenredige inspanning, vastgesteld kan worden.
De wet maakt een onderscheid in direct en indirect identificerende gegevens:

- Direct identificerende gegevens zijn gegevens die betrekking hebben op een persoon, waarvan de identiteit zonder veel omwegen eenduidig is vast te stellen, zoals een naam, eventueel in combinatie met het adres en de geboortedatum.
- Van indirect identificerende gegevens is sprake, wanneer gegevens via nadere stappen in verband kunnen worden gebracht met een bepaalde persoon.
  Een gegeven is geen persoonsgegeven, indien doeltreffende technische en organisatorische maatregelen zijn getroffen waardoor een daadwerkelijke identificatie van individuele natuurlijke personen redelijkerwijs wordt uitgesloten.

4. Definitie van een data-lek

Bij een data-lek gaat het om toegang tot persoonsgegevens of vernietiging, wijziging of vrijkomen van gegevens zonder dat dat de bedoeling is van de organisatie. Onder een data-lek valt dus niet alleen het vrijkomen (lekken) van gegevens, maar ook het onrechtmatig verwerken van gegevens. Er is sprake van een data-lek, als er inbreuk is op de beveiliging.
Bij een data-lek zijn de persoonsgegevens blootgesteld aan verlies of onrechtmatige verwerking – dus aan datgene waartegen de beveiligingsmaatregelen bescherming moeten bieden. Als er gevoelige bedrijfsinformatie wordt gelekt, dan levert dit geen meldingsplicht op.

5. Wanneer een data-lek bij de Autoriteit Persoonsgegevens melden?

Of een data-lek moet worden gemeld of niet, hangt af van de ernst van het data-lek. Het data-lek moet alleen gemeld worden als dit leidt tot ernstige nadelige gevolgen voor de bescherming van persoonsgegevens. Of als een aanzienlijke kans bestaat dat dit gebeurt.

Als we redelijkerwijs niet kunnen uitsluiten dat een inbreuk op de beveiliging tot een onrechtmatige verwerking heeft geleid, dan moet we het data-lek melden aan de Autoriteit Persoonsgegevens. En er moet bepaald worden of er sprake is van waarschijnlijk ongunstige gevolgen voor de persoonlijke levenssfeer.

Een inbreuk hoeft alleen gemeld te worden "als deze leidt tot een aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens".

5.1. Zijn er gegevens van gevoelige aard gelekt ?

Bij het beantwoorden van de vraag of er sprake is van (een aanzienlijke kans op) ernstige nadelige gevolgen voor de bescherming van de verwerkte persoonsgegevens, moeten we in ieder geval kijken naar de aard van de getroffen gegevens. Is er sprake van bijzondere persoonsgegevens of van persoonsgegevens die anderszins van gevoelige aard zijn? Bij dit laatste moeten we bijvoorbeeld denken aan gegevens over betalingsachterstanden.

Bij een aantal categorieën van persoonsgegevens, in dit kader aangeduid als persoonsgegevens van gevoelige aard, kunnen verlies of onrechtmatige verwerking onder meer leiden tot stigmatisering of uitsluiting van de betrokkene, tot schade aan de gezondheid, financiële schade of tot (identiteits)fraude.

Tot deze categorieën van persoonsgegevens moeten in ieder geval worden gerekend:

- *Bijzondere persoonsgegevens zoals bedoeld in artikel 16 Wbp*
  Het gaat hierbij om persoonsgegevens over iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, lidmaatschap van een vakvereniging en om strafrechtelijke

persoonsgegevens en persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag.

- *Gegevens over de financiële of economische situatie van de betrokkene*
  Hieronder vallen bijvoorbeeld gegevens over (problematische) schulden, salaris- en betalingsgegevens.

- *(Andere) gegevens die kunnen leiden tot stigmatisering of uitsluiting van de betrokkene*
  Hieronder vallen bijvoorbeeld gegevens over gokverslaving, prestaties op school of werk of relatieproblemen.

- *Gebruikersnamen, wachtwoorden en andere inloggegevens*
  De mogelijke gevolgen voor betrokkenen hangen af van de verwerkingen en van de persoonsgegevens waar de inloggegevens toegang toe geven. Bij de afweging moet worden betrokken dat veel mensen wachtwoorden hergebruiken voor verschillende verwerkingen.

- *Gegevens die kunnen worden misbruikt voor (identiteits)fraude*
  Het gaat hierbij onder meer om biometrische gegevens, kopieën van identiteitsbewijzen en om het burgerservicenummer (bsn).

6. Hoe melden we een data-lek intern?

1. Ontvangen van een mogelijk data-lek.
2. Na de constatering van een eventueel data-lek wordt dit direct aan de voorzitter van het bestuur.
3. Het bestuur gaat het data-lek direct onderzoeken.
4. Vervolgens beoordeelt de voorzitter het volgende:
    a. De Voorzitter beoordeeld het gerapporteerde beveiligingsincident.
    b. De Voorzitter besluit of het data-lek gemeld moet worden aan de Autoriteit Persoonsgegevens.
    c. De Voorzitter neemt het besluit of het data-lek gemeld moet worden aan de betrokkenen.
    d. De Voorzitter informeert de bestuurder over de genomen beslissing.
5. De secretaris neemt de melding op in het register datalekken.

7. Hoe melden we een data-lek bij de Autoriteit Persoonsgegevens?

De melding wordt gedaan door de voorzitter, eventueel met een extern in te huren adviseur.

De Autoriteit Persoonsgegevens stelt een webformulier beschikbaar waarmee data-lekken kunnen worden gemeld.

We mogen na het ontdekken van een mogelijk data-lek enige tijd (maximaal 72 uur) nemen voor nader onderzoek om een onnodige melding te voorkomen. Uiterlijk op de tweede werkdag na de ontdekking van het incident doen we een melding bij de AP, tenzij op dat moment al uit ons onderzoek is gebleken dat het incident niet onder de meldplicht data-lekken valt. Mogelijk hebben we op de tweede werkdag na de ontdekking van het data-lek nog niet volledig zicht op wat er gebeurd is en om welke persoonsgegevens het gaat. In dat geval doen we de melding op basis van de gegevens waarover we op dat moment beschikken. Eventueel kunnen we de melding naderhand nog aanvullen of intrekken.

We ontvangen na het melden een ontvangstbevestiging. Bij die meldingen die aanleiding geven tot nadere actie door de Autoriteit Persoonsgegevens zullen zij contact met ons opnemen om de herkomst van de melding te verifiëren.

8. Wanneer moeten we een data-lek melden bij de betrokkenen?

De betrokkenen hoeven alleen geïnformeerd te worden als een data-lek waarschijnlijk ongunstige gevolgen heeft voor hun persoonlijke levenssfeer. We kunnen hierbij denken aan bepaalde vormen van fraude of als sprake is van aantasting van iemands goede naam en reputatie.

9. Hoe melden we aan betrokkenen?

In de kennisgeving aan de betrokkene vermelden we in ieder geval: de aard van de inbreuk, de instanties waar de betrokkene meer informatie over de inbreuk kan krijgen, en de maatregelen die we de betrokkene aanbevelen om te nemen om de negatieve gevolgen van de inbreuk te beperken.

Bij het beschrijven van de aard van de inbreuk kunnen we doorgaans met een algemene omschrijving volstaan. We nemen onze contactgegevens op zodat de betrokkene ons kan bereiken als hij of zij vragen heeft over het data-lek. Verder geven we aan wat de betrokkene zelf kan doen om de negatieve gevolgen van het data-lek te beperken. We moeten daarbij denken aan het veranderen van gebruikersnamen en wachtwoorden wanneer deze door de inbreuk mogelijk gecompromitteerd zijn.

Het staat ons vrij om meer informatie toe te voegen aan de kennisgeving, maar dit is niet verplicht.
In veruit de meeste gevallen zullen we als verantwoordelijke beschikken over de contactgegevens van de betrokkenen, en zullen we in staat zijn om de betrokkenen individueel te informeren.
Bij meer omvangrijke incidenten kunnen we kiezen voor een combinatie van algemene voorlichting en het op individuele basis informeren van betrokkenen.

Het belangrijkste is, dat we zo veel mogelijk betrokkenen bereiken met informatie die hen helpt om de gevolgen van het data-lek voor hun persoonlijke levenssfeer zo veel mogelijk te beperken. Met enkel een bericht in de media wordt dat doel normaal gesproken niet bereikt.

10. Preventieve en corrigerende maatregelen

1. Het beoordelen van de noodzaak om maatregelen te treffen
   Als de oorzaak bekend is, wordt bekeken of het noodzakelijk is om corrigerende maatregelen te treffen. De beslissing om te komen tot corrigerende maatregelen dient beoordeeld te worden tijdens de vaste overleggen of tussentijds in overleg met de Voorzitter.

2. Het vaststellen en doorvoeren van de benodigde maatregelen
   Het vaststellen van de benodigde maatregelen wordt vastgelegd in notities, e-mails/brieven, verslagen, procedures, procesbeschrijvingen of rapporten. Alle betrokkenen worden geïnformeerd en verzocht te handelen zoals de maatregel aangeeft.

3. Het beoordelen van de getroffen maatregelen
   Afhankelijk van de uitslag van de beoordeling wordt vastgesteld of een herbeoordeling noodzakelijk is, of er wederom maatregelen genomen moeten worden, of dat de maatregel voldoende is geweest. Verificatie van de doeltreffendheid van maatregelen wordt gedaan bij het vaststellen van de doeltreffendheid van de afgehandelde actiepunten.

11. Register data-lekken

We hebben de verplichting om een register bij te houden van alle lekken die ernstig genoeg waren om te melden aan het Autoriteit Persoonsgegevens. Het register wordt beheerd door de secretaris.

De Voorzitter en de secretaris kunnen bij dit register.
We gaan uit van een bewaartermijn van minimaal 3 jaar.

12. Wat gebeurt er als de regels worden overtreden?

Indien een data-lek ten onrechte niet wordt gemeld bij de Autoriteit Persoonsgegevens dan kan de autoriteit een hoge geldboete geven. De maximale geldboete is theoretisch € 820.000 (hoogste categorie) of, als dat niet passend is 10% van de netto jaaromzet van de rechtspersoon. Bij een overtreding van de AVG wordt een bestuurlijke boete van de 2e categorie opgelegd (met een maximum van € 500.000).