Privacyreglement Vereniging Slow Food Nederland

1. Begripsbepalingen
1.1 *Persoonsgegeven*: een gegeven dat herleidbaar is tot een individuele natuurlijke persoon.
1.2 *Verwerking van persoonsgegevens*: elke handeling of geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, wissen en vernietigen van gegevens.
1.3 *Betrokkene*: degene op wie de persoonsgegevens betrekking hebben.
1.4 *Verwerkingsverantwoordelijke:* een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt/degene die bepaalt welke verwerking van persoonsgegevens voor welk doel plaatsvindt.
1.5 *Datalek*: 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. Hierbij kan men denken aan bijvoorbeeld het kwijtraken van een USB-stick, de diefstal van een laptop, besmetting met malware of een inbraak door een hacker.

2. Verantwoordelijkheid en coördinator
2.1 Het bestuur van de vereniging draagt collectieve verantwoordelijkheid voor de naleving van alle wettelijke regelingen inzake de verwerking van persoonsgegevens.
2.2 De secretaris van het bestuur van de vereniging is Coördinator Persoonsgegevens en zorgt voor het beheer en de verwerking van de persoonsgegevens die berusten bij de vereniging (hierna: de secretaris).
2.3 De secretaris kan de verwerking van de gegevens laten uitvoeren door een expliciet aangewezen administrateur. Is de administrateur lid van de vereniging, dan ondertekent hij vóór aanvang van de werkzaamheden een Verklaring Algemene Verordening Gegevensbescherming zoals vastgelegd in bijlage1 van dit reglement.Is de administrateur een derde partij, dat wordt met deze een verwerkersovereenkomst afgesloten, waarvan een voorbeeld is vastgelegd in bijlage 2 van dit reglement.
2.4 Gelet op de beperkte omvang van de verwerking van persoonsgegevens wordt bij de vereniging geen functionaris voor de gegevensbescherming in de zin van de AVG aangesteld.

3. Doel van de verwerking van persoonsgegevens en beheer
3.1 Door de vereniging worden gegevens verwerkt die noodzakelijk zijn voor:
a. het bijhouden van een actuele ledenlijst van de vereniging;
b. het bijhouden van actuele relatielijsten van de vereniging;
c. het financiële beheer van de vereniging;
d. de organisatie van activiteiten;
e. het samenstellen en verzenden van (elektronische) nieuwsbrieven, bladen, persberichten en bestuursmededelingen;
f. de registratie van een taken, functies of specifieke kennis van leden;
g. managementinformatie;
h. het bijhouden van het archief van de vereniging.

4. Verwerking van persoonsgegevens en het beheer
4.1 Door de vereniging worden de volgende persoonsgegevens verwerkt:
a. voornaam, voorletters, achternaam en voorvoegsel(s);
b. straatnaam, huisnummer, postcode en plaats;
c. telefoonnummer(s) en e-mailadres(sen);

d. aanspreekvorm;
e. bedrijf en/of beroep;
f. Iban-nummers ingeval van automatische incasso's of het versturen van acceptgiro's;
g. gegevens over door betrokkene betaalde contributies, donaties en/of sponsorcontracten over het lopende jaar en maximaal zeven daaraan voorafgaande jaren;
3.2 Betreft het persoonsgegevens van ingeschreven leden van de vereniging, dan worden bovendien de volgende persoonsgegevens verwerkt:
h. geboortedatum;
i. lidmaatschapsvorm en aanvangsdatum lidmaatschap;
j. de community waar het desbetreffende lid is ingeschreven;
k. tijdens activiteiten gemaakte foto's en video's waarop aan die activiteiten deelnemende leden staan afgebeeld;
4.2 In het Register Verwerkingen Persoonsgegevens wordt door de secretaris vastgelegd welke types persoonsgegevens door de vereniging worden verwerkt. Een registeropzet is vastgelegd in bijlage 3 bij dit reglement.
4.3 Voor de verwerking van persoonsgegevens wordt gebruik gemaakt van een administratief systeem voor gegevensverwerking, dat voor de vereniging is ontwikkeld door het bedrijf All United B.V.
4.4 Voor de verzending van elektronische nieuwsbrieven en bestuursmededelingen wordt gebruikt gemaakt van online programma's voor nieuwsbrieven en mailings.
4.5 Jaarlijks wordt in het Bestuursverslag opgegeven van welke programma's gebruik is gemaakt voor de in de voorgaande leden bedoelde activiteiten.
4.6 Het archief van de vereniging betreft een digitale kluis bij het bedrijf All United B.V.

5. Toegang tot persoonsgegevens
5.1 Toegang tot (delen van) de persoonsgegevens hebben:
a. bestuursleden van de vereniging;
b. individuele leden en commissies die zijn belast met de organisatie van activiteiten;
c. medewerkers van de vereniging voor zover hun taak de omgang met persoonsgegevens met zich meebrengt;
d. (bestuurs)leden van communities die door hun community gemachtigd zijn.
5.2 Alle in 5.1. genoemde personen ondertekenen voorafgaand aan de toegang tot de gegevens de Verklaring Algemene Verordening Gegevensbescherming, zoals vastgelegd in bijlage 1 bij van dit reglement.
5.3 Behoudens het bepaalde in de voorgaande leden en artikel 6.4 hebben derden - daaronder mede begrepen andere verenigingsleden dan de betrokkene zelf – geen toegang tot of inzage in de door de vereniging verwerkte persoonsgegevens, tenzij derden op grond van een afgesloten verwerkersovereenkomst verwerking van persoonsgegevens is toegestaan, dan wel aan derden op basis van hun wettelijke bevoegdheden toegang of inzage moet worden verleend.
5.4 Jaarlijks wordt in het Bestuursverslag opgegeven welke personen of bedrijven toegang hebben gekregen tot de in dit reglement bedoelde persoonsgegevens.

6. Publicatie van persoonsgegevens
6.1 De vereniging onderhoudt een website. Op de website publiceert de vereniging een privacyverklaring, inhoudende het verenigingsbeleid met betrekking tot de aan haar toevertrouwde persoonsgegevens en een verwijzing naar het geldende privacyreglement.
6.2 De vereniging communiceert met haar leden via nieuwsbrieven, magazines en bestuursmededelingen. In deze nieuwsbrieven en magazines kunnen foto's of video's worden gepubliceerd van door de vereniging georganiseerde activiteiten, waarop aan die activiteiten deelnemende leden staan afgebeeld en eventueel met name genoemd worden.
6.3 De vereniging onderhoudt onder andere accounts op Facebook, Twitter en Instagram (hierna: social media). Op deze social media kunnen teksten, foto's of video's worden gepubliceerd waarop leden staan afgebeeld en met name genoemd. Persoonsgegevens anders dan naamgegevens van betrokkene worden uitsluitend middels een link naar het betreffende eigen account van betrokkene op deze social media gepubliceerd.
6.4 Betrokkenen kunnen bezwaar maken tegen de publicatie van foto's en video's en/of de vermelding van hun naam op de social media accounts van de vereniging. Artikel 9 van dit reglement regelt de manier van bezwaar maken.
6.5 Persoonsgegevens van verenigingsleden, dan wel delen daarvan, kunnen ter beschikking worden gesteld aan derden, daaronder mede begrepen andere verenigingsleden dan de betrokkene zelf. Wie wil beschikken over persoonsgegevens dient daartoe een gemotiveerde aanvraag in bij de secretaris van de vereniging [e-mail:secretaris@slowfood.nl]. Binnen twee weken na ontvangst van de aanvraag bericht de secretaris de aanvrager schriftelijk of, dan wel in hoeverre, aan het verzoek kan worden

voldaan. Een weigering is met redenen omkleed. De secretaris beslist of de ter beschikkingstelling van persoonsgegevens niet eerder zal plaatsvinden dan na toestemming van betrokkenen.
6.6 Foto's en video's waarop verenigingsleden herkenbaar zijn, kunnen niet ter beschikking van derden - daaronder mede begrepen andere verenigingsleden dan de betrokkene zelf - worden gesteld, anders dan na toestemming van betrokkene.
6.7 Persoonsgegevens van relaties anders dan leden van de vereniging kunnen pas ter beschikking van derden - daaronder mede begrepen verenigingsleden - worden gesteld na toestemming van betrokkene. Foto's en video's waarop deze relaties - dan wel natuurlijke personen werkzaam bij deze relaties - herkenbaar zijn, kunnen pas na toestemming van betrokkene worden gepubliceerd.

7. Inzage in eigen persoonsgegevens
7.1 Betrokkene heeft recht op inzage in en afschrift van de op zijn persoon betrekking hebbende gegevens. Betrokkene kan daartoe op de website van de vereniging -via een aanmeldingsprocedure- de eigen persoonsgegevens oproepen.
7.2 Daarnaast kan betrokkene een verzoek tot inzage in eigen persoonsgegevens indienen bij de secretaris of de gemachtigde administrateur (e-mail: administratie@slowfood.nl). Aan zo'n verzoek wordt binnen twee weken na ontvangst voldaan.
7.3 Het recht op inzage wordt alleen toegestaan aan betrokkene of diens gemachtigde. Betrokkene of diens gemachtigde moeten zich op aanvraag kunnen legitimeren.
7.4 Het bestuur kan weigeren aan een verzoek als bedoeld in dit artikel te voldoen voor zover dit noodzakelijk is in het belang van de bescherming van betrokkene of van de rechten en vrijheden van anderen.
7.5 Voor de verstrekking en verzending van afschriften worden geen kosten in rekening gebracht.
7.6 Een verzoek van betrokkene tot overdracht van zijn persoonsgegevens aan een andere organisatie wordt gelijkgesteld met het recht op inzage in eigen persoonsgegevens en op dezelfde wijze behandeld.

8. Aanvulling, correctie of verwijdering van opgenomen gegevens
8.1 Betrokkene heeft recht op aanvulling of correctie van opgenomen gegevens. Betrokkene kan daartoe op de website van de vereniging -via een aanmeldingsprocedure- de eigen persoonsgegevens veranderen. Een verwijdering van de totale gegevens kan niet via de website doorgevoerd worden.
8.2 Daarnaast kan betrokkene een verzoek tot aanvulling, correctie of verwijdering indienen bij de secretaris of de gemachtigde administrateur (e-mail: administratie@slowfood.nl).
8.3 Desgevraagd worden de opgenomen gegevens aangevuld met een door betrokkene afgegeven verklaring met betrekking tot de opgenomen gegevens.
8.4 Binnen twee weken na ontvangst bericht de secretaris of de gemachtigde administrateur de betrokkene schriftelijk of, dan wel in hoeverre, aan het verzoek zal worden voldaan. Een weigering is met redenen omkleed.
8.5 Verwijdering blijft achterwege voor zover bewaring op grond van een wettelijk voorschrift is vereist.
8.6 In geval van verwijdering van gegevens wordt in de administratie een verklaring opgenomen dat de gegevens op verzoek van betrokkene zijn verwijderd.
8.7 Verwijdering van persoonsgegevens kan er toe leiden dat voortzetting van het lidmaatschap van de vereniging niet meer mogelijk is. De betreffende persoon wordt hierover geïnformeerd.

9. Klachtenregeling
9.1 Klachten over de verwerking van persoonsgegevens kunnen door betrokkene of diens gemachtigde schriftelijk worden ingediend bij de secretaris van het bestuur. De secretaris bevestigt de ontvangst van de klacht aan betrokkene of diens gemachtigde met vermelding van het vervolg van de procedure.
9.2 Komt de secretaris tot de conclusie dat volledig aan de klacht kan worden tegemoet gekomen dan kan hij een daartoe strekkend voorstel doen aan de klager. Aanvaardt de klager die oplossing, dan is de klacht daarmee afgedaan en wordt de procedure van de artt. 9.3 tot en met 9.4 niet gevolgd.
9.3 Indien handelen of nalaten van de secretaris (mede) aanleiding lijkt te hebben gegeven tot de klacht, wordt de behandeling van de klacht overgedragen aan de voorzitter van het bestuur of bij diens ontstentenis een aangewezen plaatsvervanger, niet zijnde de secretaris.
9.4 De secretaris of diens plaatsvervanger formeert een commissie van drie personen die gezamenlijk de klacht beoordelen. De betrokkene heeft het recht door deze commissie te worden gehoord.
9.5 Binnen zes weken na ontvangst van de klacht bericht de secretaris of diens plaatsvervanger de betrokkene schriftelijk of, dan wel in hoeverre, aan de klacht tegemoet zal worden gekomen. De beslissing is met redenen omkleed.
9.6 Deze klachtenregeling beperkt niet de juridische mogelijkheden van betrokkene op grond van wet en regelgeving.

10. Bewaartermijn
10.1 Persoonsgegevens worden niet langer bewaard dan noodzakelijk is voor de verwerkelijking van de doeleinden waarvoor zij zijn verzameld.
10.2 De in het in artikel 4.4 bedoelde online programma voor nieuwsbrieven en mailings opgeslagen foto's en video's, waarop leden van de vereniging staan afgebeeld, worden na verloop van één jaar uit dat programma verwijderd.
10.3 De (digitale) aanmeldings- en presentielijsten van door de vereniging georganiseerde activiteiten – met uitzondering van de presentielijsten van de Algemene Ledenvergaderingen - worden binnen een maand na afloop van de betreffende activiteiten vernietigd.
10.4 De persoonsgegevens van betrokkene – niet zijnde tijdens activiteiten gemaakte foto's en video's waarop hij of zij staat afgebeeld - worden binnen twee jaar na overlijden of opzegging van het lidmaatschap verwijderd, tenzij sprake is van een wettelijke bewaartermijn[1].

11. Beveiliging van persoonsgegevens.
11.1 Iedereen die toegang tot persoonsgegevens krijgt conform art. 5, heeft van de secretaris voorlichting ontvangen over het beveiligen van ledengegevens en heeft het Privacyreglement gelezen. Daarnaast heeft elke verantwoordelijke vóór inzage van de gegevens een Verklaring Algemene Verordening Gegevensbescherming zoals vastgelegd in bijlage1 van dit reglement, ondertekend.
11.2 De persoonsgegevens van de vereniging zijn vastgelegd in de administratie bij All United B.V. Toegang tot de administratie onderligt de veiligheidsinstellingen van All United B.V. en zijn na te lezen op de website van All United B.V. (https://www.allunited.nl/privacy-veiligheid).
11.3 De persoonsgegevens die zijn vastgelegd in het programma voor mailings en nieuwsbrieven betreffen uitsluitend naam en e-mailadres en zijn uitsluitend toegankelijk na autorisatie door de secretaris en een vastgelegde inlogprocedure.
11.3 Indien op enig moment sprake is van een (mogelijk) datalek wordt daarvan onmiddellijk melding gedaan aan de secretaris van het bestuur.
11.4 de secretaris verwerkt het opgetreden (mogelijk) datalek conform het Protocol Datalekken, vastgelegd in bijlage 4 van dit reglement.
11.5 Aan het begin van elk kalenderjaar worden de beheers/beveiligingsmaatregelen en de naleving van de AVG door het bestuur geëvalueerd.

12. Inwerkingtreding en toepassingsgebied
12.1 Dit reglement treedt in werking op 16 juni 2018.
12.2 Het reglement is van toepassing op iedere verwerking van persoonsgegevens van leden en relaties van de vereniging in de zin van de Algemene EU-Verordening Gegevens-bescherming (AVG).
12.3 Dit reglement bevat vier bijlagen, die integraal onderdeel zijn van dit reglement.

[1] Bewaartermijnen zijn onder andere geregeld in de Algemene wet inzake rijksbelastingen: op grond van artikel 52 van die wet heeft een vereniging de verplichting om haar boekhouding en haar algemene administratie 7 jaar te bewaren; zie ook artikel 4.1, onder h.

Bijlage 1 van het privacyreglement Slow Food Nederland

Verklaring Algemene Verordening Gegevensbescherming

Uitleg:
Te tekenen door iedereen die toegang heeft tot enige deel van de bij de organisatie berustende persoonsgegevens.
NB: ook betalingsgegevens zijn persoonsgegevens, voor zover ze (banknummer) te herleiden zijn tot een natuurlijke persoon.

[naam betrokken medewerker/bestuurslid] verklaart hierbij

- Dat hij/zij zich realiseert, dat zijn functie bij de Vereniging Slow Food Nederland meebrengt dat hij/zij toegang heeft tot persoonsgegevens van de Vereniging Slow Food Nederland [en deze gegevens kan aanpassen en/of verwijderen];
- Dat hij/zij op de hoogte is van het feit, dat ingevolge de Algemene Verordening Gegevensbescherming en de Uitvoeringswet Algemene Verordening Gegevensbescherming **("AVG"**) zorgvuldig moet worden omgegaan met persoonsgegevens, welke zorgvuldigheid onder meer vereist, dat persoonsgegevens in beginsel niet aan derden ter beschikking worden gesteld, dat fouten erin moeten worden gecorrigeerd en dat bestanden van persoonsgegevens naar de stand der techniek moeten worden beveiligd tegen toegang door onbevoegden;
- Dat de AVG een organisatie bij wie persoonsgegevens berusten, verplicht tot het treffen van maatregelen wanneer (er een vermoeden bestaat, dat) onbevoegden toegang hebben gekregen (/dreigen te krijgen) tot die persoonsgegevens **("datalek")**
- Dat hij/zij een afschrift heeft ontvangen en heeft kennis genomen heeft van het privacyreglement van de Vereniging Slow Food Nederland ten aanzien van persoonsgegevens en de privacyverklaring die de Vereniging Slow Food Nederland op haar website heeft geplaatst;
- Dat hij/zij zich zal inspannen om de in de AVG, het privacybeleid van de Vereniging Slow Food Nederland en het privacyreglement van de Vereniging Slow Food Nederland vervatte regels en gedragslijnen steeds te respecteren en het direct zal melden bij de secretaris van het bestuur van de Vereniging Slow Food Nederland wanneer hij/zij een redelijk vermoeden heeft, dat sprake is van een datalek of een andere overtreding van deze regels en gedragslijnen plaatsvindt of dreigt, onverschillig of die het gevolg is van eigen handelen of nalaten of van handelen of nalaten door een of meer derden, binnen of buiten de organisatie.

[Plaats, datum]

[Naam]
[Functie]

Bijlage 2 van het privacyreglement Slow Food Nederland

Verwerkersovereenkomst

Partijen

De Vereniging Slow Food Nederland gevestigd aan de <adres> te <plaatsnaam>, verder te noemen de verwerkingsverantwoordelijke, te dezen rechtsgeldig vertegenwoordigd door de <heer/mevrouw> <naam>.
en
[naam verwerker] gevestigd aan de <adres> te <plaatsnaam>, verder te noemen de verwerker, ten deze rechtsgeldig vertegenwoordigd door de <de heer of mevrouw>, <persoonsnaam> , <functie>,
(hierna afzonderlijk ook aangeduid als "partij" en gezamenlijk als "partijen") verklaren te zijn overeengekomen een verwerkersovereenkomst als bedoeld in artikel 14 tweede lid van de Wet Bescherming persoonsgegevens en, vanaf 25 mei 2018, als bedoeld in artikel 28, derde lid, van de Algemene Verordening Gegevensbescherming (hierna: AVG), tussen de verwerkingsverantwoordelijke en de verwerker. Waar in deze verwerkersovereenkomst termen worden gebruikt die overeenstemmen met definities uit artikel 4 AVG, wordt aan deze termen de betekenis van de definities uit de AVG toegekend.

Artikel 1 Definities

1.1 Bijlagen: aanhangsels bij deze verwerkersovereenkomst, die na door partijen te zijn geparafeerd, deel uitmaken van deze verwerkersovereenkomst.

1.2 Incident: afwijking van de normale gang van zaken bij de verwerking van persoonsgegevens met mogelijk negatieve gevolgen, zoals geconstateerde of vermoede ongeautoriseerde of onrechtmatige verwerking, verwijdering en verlies van persoonsgegevens, datalekken in de zin van artikel 33 AVG alsmede inbreuken op de beveiliging, geheimhouding of integriteit van systemen, infrastructuur en/of Persoonsgegevens

1.3. Normen en standaarden: de door de verwerkingsverantwoordelijke vastgestelde normen en standaarden ter zake van methoden, technieken, procedures, projecten, productiekenmerken en documentatievoorschriften welke bij de uitvoering van de werkzaamheden door de verwerker zullen worden gevolgd als vastgelegd in bijlage 1.

1.4 Toezichthouder: de Autoriteit Persoonsgegevens (AP).

1.5. (Verwerkings)verantwoordelijke: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt, in dit geval

1.6. Verwerker: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt. In dit geval <naam verwerker>. Degene die ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt, in opdracht van de verwerker, is een sub-verwerker.

Artikel 2 Ingangsdatum en duur

2.1 Deze verwerkersovereenkomst gaat in op het moment van ondertekening en duurt voort zolang de verwerker als verwerker van persoonsgegevens optreedt in het kader van de door de verwerkingsverantwoordelijke ter beschikking gestelde persoonsgegevens voor <beschrijving activiteit(en)>

Artikel 3 Onderwerp van deze verwerkersovereenkomst

3.1 De verwerker verwerkt de door of via verwerkingsverantwoordelijke ter beschikking gestelde persoonsgegevens uitsluitend in opdracht van de verwerkingsverantwoordelijke in het kader van de uitvoering van <contract, nummer>; dit is de onderliggende hoofdovereenkomst. De door de verwerker uit te voeren verwerking en werkzaamheden waar deze verwerkersovereenkomst betrekking op heeft, evenals het doel van de verwerking, worden nader, uitputtend, omschreven in bijlage 2. Verwerker zal de persoonsgegevens niet voor enig ander doel verwerken, behoudens afwijkende wettelijke verplichtingen.

3.2 De verwerker verbindt zich om de in het kader van die werkzaamheden door of via de verwerkingsverantwoordelijke ter beschikking gestelde persoonsgegevens (**"de Persoonsgegevens"**) zorgvuldig te verwerken.

Artikel 4 Verplichtingen verwerker

4.1 De verwerker verwerkt de Persoonsgegevens ten behoeve van de verwerkingsverantwoordelijke in overeenstemming met diens schriftelijke instructies.

4.2 De verwerker heeft geen zeggenschap over de Persoonsgegevens. Zo neemt hij geen beslissingen over ontvangst en gebruik van de Peroonsgegevens, de verstrekking aan derden en de duur van de opslag ervan. De zeggenschap over de Persoonsgegevens komt nimmer bij de verwerker te berusten.

4.3 De verwerker zal bij de verwerking van de Persoonsgegevens handelen in overeenstemming met de toepasselijke wet- en regelgeving. De verwerker zal alle redelijke instructies van de contactpersoon, ais bedoeld in artikel 12.2, opvolgen tenzij die in strijd komen met wettelijke verplichtingen. In dat laatste geval stelt de verwerker de verantwoordelijke vooraf op de hoogte.

4.4 De verwerker stelt op eerste verzoek van de contactpersoon (artikel 12.2), door verwerkingsverantwoordelijke ter beschikking gestelde persoonsgegevens met betrekking tot deze verwerkersovereenkomst ter hand stellen.

4.5 De verwerker stelt de verwerkingsverantwoordelijke te allen tijde in staat om binnen de wettelijke termijnen te voldoen aan de verplichtingen op grond van de AVG zoals verzoeken van betrokkenen om inzage, verbetering, aanvulling, verwijdering of afscherming van persoonsgegevens en het handelen naar aanleiding van de honorering van een bezwaar van een betrokkene.

4.6 De verwerker werkt op verzoek van verwerkingsverantwoordelijke te allen tijde mee aan een gegevensbeschermingseffectbeoordeling (PIA).

Artikel 5 Geheimhoudingsplicht

5.1 De verwerker en de personen in dienst van, dan wel werkzaam voor de verwerker zijn verplicht tot geheimhouding van de Persoonsgegevens behoudens en voor zover een bij, of krachtens de wet gegeven voorschrift tot verstrekking verplicht. De medewerkers van de verwerker tekenen hiertoe een geheimhoudingsverklaring.

5.2 Indien de verwerker op grond van een wettelijke verplichting gegevens dient te verstrekken, zal de verwerker (i) de grondslag van het verzoek en de identiteit van de verzoeker verifiëren en (ii) de verwerkingsverantwoordelijke onmiddellijk, voorafgaand aan de verstrekking, ter zake informeren tenzij wettelijke bepalingen dat verbieden.

Artikel 6 Meldplicht datalekken en beveiligingsincidenten

6.1 De verwerker zal de verwerkingsverantwoordelijke zo spoedig mogelijk - doch uiterlijk binnen 24 uur na de eerste ontdekking - informeren over alle (vermoedelijke) incidenten, zoals inbreuken op de beveiliging die op grond van wetgeving moeten worden gemeld aan de toezichthouder of betrokkene, onverminderd de verplichting de gevolgen van dergelijke inbreuken en incidenten zo snel mogelijk ongedaan te maken dan wel te beperken, al dan niet onder verbeurte van een boete in geval van niet-nakoming, conform artikel 10.4 van deze verwerkersovereenkomst. Verwerker zal voorts, op eerste verzoek van de verwerkingsverantwoordelijke, alle inlichtingen verschaffen die de verwerkingsverantwoordelijke noodzakelijk acht om het incident te kunnen beoordelen. Daartoe behoort in ieder geval de informatie zoals omschreven in bijlage 3.

6.2 De verwerker beschikt over een plan van aanpak betreffende inbreuken en zal de verwerkingsverantwoordelijke, op diens verzoek, inzage verschaffen in het plan van aanpak. Verwerker stelt de verwerkingsverantwoordelijke op de hoogte van materiele wijzigingen in het plan van aanpak.

6.3 De verwerker zal het doen van meldingen aan de toezichthouder(s) overlaten aan de verwerkingsverantwoordelijke.

6.4 De verwerker zal alle noodzakelijke medewerking verlenen aan het zo nodig, op de kortst mogelijke termijn, verschaffen van aanvullende informatie aan de toezichthouder(s) en/of betrokkene(n). Daarbij verschaft verwerker in ieder geval de informatie, zoals beschreven in bijlage 3, aan de verwerkingsverantwoordelijke.

6.5 De verwerker houdt een logboek bij van de (vermoedens van) inbreuken op de beveiliging en daarop genomen maatregelen . Het bevat minimaal de informatie van bijlage 3. De verwerker geeft de verwerkingsverantwoordelijke op eerste verzoek inzage in dat logboek.

Artikel 7 Beveiligingsmaatregelen en controle

7.1 De verwerker neemt alle passende technische en organisatorische maatregelen om de Persoonsgegevens te beveiligen en beveiligd te houden tegen verlies of tegen enige vorm van onrechtmatige verwerking. De wijze van beveiliging wordt nader omschreven in bijlage 4.

7.2 De verwerkingsverantwoordelijke is te allen tijde gerechtigd de verwerking van persoonsgegevens te (doen) controleren. De verwerker is verplicht de verwerkingsverantwoordelijke, de Autoriteit Persoonsgegevens, of, de onder geheimhouding controlerende instantie in opdracht van verwerkingsverantwoordelijke toe te laten en de voor de controle verder noodzakelijke medewerking te verlenen.

7.3 De verwerkingsverantwoordelijke zal de verwerker op voorhand schriftelijk op de hoogte stellen van een controle.

7.4 De verwerker verbindt zich om binnen een door de verwerkingsverantwoordelijke te bepalen termijn de verwerkingsverantwoordelijke, of een door de verwerkingsverantwoordelijke ingeschakelde derde te voorzien van informatie die de verwerkingsverantwoordelijke, of die derde nodig heeft om zich een oordeel te vormen over de naleving door de verwerker van deze verwerkersovereenkomst. De verwerkingsverantwoordelijke, of deze derde behandelt alle informatie betreffende deze controles vertrouwelijk.

7.5 Verwerker voert de door de verwerkingsverantwoordelijke of de ingeschakelde derde gedane aanbevelingen uit binnen de daartoe door de verwerkingsverantwoordelijke bepaalde redelijke termijn.

7.6 De verwerker rapporteert jaarlijks over de opzet en werking van de maatregelen en procedures gericht op naleving van deze verwerkersovereenkomst.

7.7 Naast rapportages door de verwerker en controles door de verwerkingsverantwoordelijke of controlerende instantie in opdracht van de verwerkingsverantwoordelijke, kunnen partijen ook overeenkomen gebruik te maken van een Third Party Memorandum (TPM) opgesteld door een onafhankelijke externe deskundige.

7.8 De redelijke kosten van de controle worden gedragen door de partij die de kosten maakt, tenzij uit de controle blijkt dat de verwerker enig punt uit deze verwerkersovereenkomst niet heeft nageleefd in welk geval de kosten van de controle worden gedragen door de verwerker.

Artikel 8 Inschakeling derden

8.1 De verwerker is slechts gerechtigd de uitvoering van de werkzaamheden geheel of ten dele uit te besteden aan derden na voorafgaande, duidelijk gespecificeerde, schriftelijke toestemming van de verwerkingsverantwoordelijke.

8.2 De verwerkingsverantwoordelijke kan aan de schriftelijke toestemming voorwaarden verbinden, op het gebied van geheimhouding en ter naleving van de verplichtingen uit deze verwerkersovereenkomst.

8.3 De verwerker blijft in deze gevallen te allen tijde aanspreekpunt en verantwoordelijk voor de naleving van de bepalingen uit deze verwerkersovereenkomst. De verwerker garandeert dat deze derden schriftelijk minimaal dezelfde plichten op zich nemen als tussen de verwerkingsverantwoordelijke en de verwerker zijn overeengekomen en zal de verwerkingsverantwoordelijke, op diens verzoek, inzage verschaffen in de overeenkomsten met deze derden waarin deze plichten zijn opgenomen.

8.4 De verwerker mag de persoonsgegevens uitsluitend verwerken in Nederland. Doorgifte naar andere landen is uitsluitend toegestaan na voorafgaande schriftelijke toestemming van de verwerkingsverantwoordelijke en met inachtneming van de toepasselijke wet- en regelgeving.

8.5 De verwerker houdt een actueel register bij van de door hem ingeschakelde derden en onderaannemers waarin de identiteit, vestigingsplaats en een beschrijving van de werkzaamheden van de derden of onderaannemers zijn opgenomen, alsmede eventuele door de verwerkingsverantwoordelijke gestelde aanvullende voorwaarden. Dit register zal als bijlage 5 aan deze verwerkersovereenkomst worden toegevoegd en zal door de verwerker actueel worden gehouden.

Artikel 9 Wijziging en beëindigen verwerkersovereenkomst

9.1 Wijziging en aanvulling van deze verwerkersovereenkomst kunnen slechts schriftelijk plaatsvinden, middels een door partijen geaccordeerde tekst.

9.2 Zodra de samenwerking is beëindigd, zal de verwerker naar keuze van de verwerkingsverantwoordelijke (i) alle of een door verwerkingsverantwoordelijke bepaald gedeelte van haar in het kader van deze verwerkersovereenkomst ter beschikking gestelde persoonsgegevens aan de verwerkingsverantwoordelijke ter beschikking stellen (ii) de persoonsgegevens die hij van de verwerkingsverantwoordelijke heeft ontvangen op alle locaties vernietigen, in welke vorm dan ook en toont dit aan, tenzij partijen iets anders overeenkomen. De verantwoordelijk kan zo nodig nadere eisen stellen aan de wijze van beschikbaarstelling, waaronder eisen aan het bestandsformaat, dan wel vernietiging. Deze werkzaamheden moeten, binnen nader overeen te komen redelijke termijn, uitgevoerd worden en hiervan wordt een verslag gemaakt.

9.3 De verwerker zal te allen tijde de in het vorig lid beschreven recht op overdraagbaarheid van gegevens conform artikel 20 AVG waarborgen, zodanig dat er geen sprake is van verlies van functionaliteit of (delen van) de gegevens.

9.4 Verwerkingsverantwoordelijke en verwerker treden met elkaar in overleg over wijzigingen in deze verwerkersovereenkomst als een wijziging in regelgeving of een wijziging in de uitleg van regelgeving daartoe aanleiding geven.

9.5 Indien een partij tekortschiet in de nakoming van een verplichting uit deze overeenkomst, kan de andere partij haar in gebreke stellen waarbij de nalatige partij alsnog een redelijke termijn voor de nakoming wordt gegund. Blijft nakoming ook dan uit dan is de nalatige partij in verzuim. Ingebrekestelling is niet nodig wanneer voor de nakoming een fatale termijn geldt, nakoming

blijvend onmogelijk is of indien uit een mededeling dan wel de houding van de andere partij moet worden afgeleid dat deze in de nakoming van haar verplichting zal tekortschieten.

9.6 De verwerkingsverantwoordelijke is gerechtigd, onverminderd hetgeen daartoe bepaald is in de verwerkersovereenkomst en de daarmee samenhangende hoofdovereenkomst, en onverminderd hetgeen overigens in de wet is bepaald, de uitvoering van deze verwerkersovereenkomst door middel van een aangetekend schrijven op te schorten, dan wel zonder rechterlijke tussenkomst met onmiddellijke ingang geheel of gedeeltelijk te ontbinden, nadat verwerkingsverantwoordelijke een of meer van de volgende situaties vaststelt:

a) verwerker vraagt (voorlopige) surseance van betaling aan;
b) verwerker vraagt zijn faillissement aan of geraakt in staat van faillissement;
c) de onderneming van verwerker wordt ontbonden;
d) verwerker staakt zijn onderneming;
e) er is sprake van een ingrijpende wijziging in de zeggenschap over de activiteiten van de onderneming van verwerker die maakt dat van de verwerkingsverantwoordelijke redelijkerwijze niet kan worden verwacht dat zij de verwerkersovereenkomst in stand houdt;
f) op een aanmerkelijk deel van het vermogen van verwerker wordt (door een andere dan de verwerkingsverantwoordelijke) beslag gelegd;
g) de andere partij schiet aantoonbaar tekort in de nakoming van de verplichtingen die voortvloeien uit deze verwerkersovereenkomst en die ernstige toerekenbare tekortkoming is niet binnen 30 dagen hersteld na een daartoe strekkende schriftelijke ingebrekestelling dan wel een van de overige situaties bedoeld in artikel 9.5 zich voordoet.

9.7 Verwerker informeert de verwerkingsverantwoordelijke indien faillissement dan wel surséance van betaling dreigt, zodat de verwerkingsverantwoordelijke tijdig kan beslissen de persoonsgegevens terug te vorderen alvorens faillissement wordt uitgesproken.

9.8 Verwerkingsverantwoordelijke is gerechtigd deze verwerkersovereenkomst en de hoofdovereenkomst per direct te ontbinden indien verwerker te kennen geeft niet (langer) te kunnen voldoen aan de betrouwbaarheidseisen die op grond van ontwikkelingen in de wet en/of de rechtspraak aan de verwerking van de persoonsgegevens worden gesteld.

9.9 Indien de verwerkersovereenkomst voortijdig wordt beëindigd is artikel 9 leden 2 en 3 van overeenkomstige toepassing.

Artikel 10 Aansprakelijkheid

10.1 Indien de verwerker tekortschiet in de nakoming van de verplichting uit deze verwerkersovereenkomst kan verwerkingsverantwoordelijke hem in gebreke stellen. Verwerker is echter onmiddellijk in gebreke als de nakoming van desbetreffende verplichting anders dan door overmacht binnen de overeengekomen termijn, reeds blijvend onmogelijk is. Ingebrekestelling geschiedt schriftelijk, waarbij aan de verwerker een redelijke termijn wordt gegund om alsnog haar verplichtingen na te komen. Deze termijn is een fatale termijn. Indien nakoming binnen deze termijn uitblijft, is verwerker in verzuim.

10.2 Verwerker is aansprakelijk op grond van het bepaalde in artikel 82 AVG, voor schade of nadeel voortvloeiende uit het niet nakomen van deze verwerkersovereenkomst, daaronder begrepen wanneer bij de verwerking niet wordt voldaan aan de specifiek tot verwerkingsgerichte verplichtingen van de AVG, of buiten de rechtmatige instructies van verwerkingsverantwoordelijke is gehandeld.

10.3 Verwerker vrijwaart verwerkingsverantwoordelijke voor schade of nadeel voor zover ontstaan door werkzaamheid van de verwerker.

10.4 Indien verwerker de in artikel 6 lid 1 neergelegde verplichting niet of niet-tijdig nakomt en de toezichthouder de verwerkingsverantwoordelijke dientengevolge een bestuurlijke boete oplegt,

is verwerker jegens de verwerkingsverantwoordelijke daarvoor aansprakelijk en kan de verwerkingsverantwoordelijke de verwerker een contractuele boete ter hoogte van maximaal het bedrag van de boete. Deze boete is niet vatbaar voor verrekening en opschorting en laat de rechten van verwerkingsverantwoordelijken op nakoming en schadevergoeding onverlet.

Artikel 11 Toepasselijk recht

11. Op deze verwerkersovereenkomst en op alle geschillen die daaruit voortvloeien of daarmee samenhangen is het Nederlands recht van toepassing.

Aldus in tweevoud opgesteld en getekend de dato
Namens de verwerkingsverantwoordelijke, <naam> van de Vereniging Slow Food Nederland,

Namens de <nader in te vullen gegevens verwerker>
<nader in te vullen gegevens vertegenwoordiger verwerker, zoals genoemd in de aanhef>

Bijlage 1: Beschrijving beveiliging ter uitwerking van artikel 1.3

In te vullen door de verwerker

1. Normenstelsel
   a. De informatiebeveiliging vindt plaats volgens algemeen erkende normen, namelijk: *(vermeld normenstelsel, zoals bijvoorbeeld NEN7510, NEN/ISO 27001, PCI/DSS)*
2. De toereikendheid van de informatiebeveiliging blijkt uit:
   a. Certificering;
   b. Periodieke externe controles zoals audits of TPM's (bijv. ISAE3xxx SOC type II);
   c. Een Assurance rapport met conclusie over de bevindingen van de auditor;
   d. Eigen controles of eigen mededelingen.
3. Uit de certificering of periodieke externe controles of uit de audits of uit de eigen controles blijkt of kan afgeleid worden dat de beveiliging voldoet aan of gelijkwaardig is met de toelichting (bijlage 4) en de daarin omschreven elementen.

Bijlage 2: Omschrijving verwerking, werkzaamheden en doel ter uitwerking van artikel 3.1.

1. De verwerker verwerkt persoonsgegevens <omschrijving activiteit>.
2. Het doel van deze verwerking is <doel verwerking>.
3. De werkzaamheden van de verwerker zijn:
   Bijvoorbeeld:
   - Hosting bestaande uit activiteiten zoals…
   - Back-ups maken en restoren
   - Applicatiebeheer bestaande uit activiteiten zoals…
   - Technisch beheer bestaande uit activiteiten zoals…
   - Database beheer bestaande uit activiteiten zoals…
   - Communicatievoorziening (zoals berichtenverkeer)
   - Archiefbeheer
4. De verwerking heeft betrekking op <omschrijving betrokkenen>. De persoonsgegevens die door de verwerker verwerkt worden zijn:
   Bijvoorbeeld:
   - NAW-gegevens
   - Bankgegevens
   - Huurovereenkomst

Bijlage 3: Inlichtingen om incidenten te beoordelen ter uitwerking van art. 6 lid 1 en 5

De verwerker zal alle inlichtingen verschaffen die de verwerkingsverantwoordelijke noodzakelijk acht om het incident te kunnen beoordelen. Daarbij verschaft verwerker in ieder geval de volgende informatie aan de verwerkingsverantwoordelijke:

- contactgegevens voor de opvolging van de melding;
- wat de (vermeende) oorzaak is van de inbreuk;
- wat het (vooralsnog bekende en/of te verwachten) gevolg is;
- wat de (voorgestelde) oplossing is;
- aantal personen waarvan gegevens betrokken zijn bij de inbreuk (indien geen exact aantal bekend is: het minimale en maximale aantal personen waarvan gegevens betrokken zijn bij de inbreuk);
- een omschrijving van de groep personen van wie gegevens betrokken zijn bij de inbreuk;
- het soort of de soorten persoonsgegevens die betrokken zijn bij de inbreuk;
- de datum waarop de inbreuk heeft plaatsgevonden (indien geen exacte datum bekend is: de periode waarbinnen de inbreuk heeft plaatsgevonden);
- de datum en het tijdstip waarop de inbreuk bekend is geworden bij verwerker of bij een door hem ingeschakelde derde of onderaannemer;
- of de gegevens versleuteld, gehasht of op een andere manier onbegrijpelijk of ontoegankelijk zijn gemaakt voor onbevoegden;
- wat de reeds ondernomen maatregelen zijn om de inbreuk te beëindigen en om de gevolgen van de inbreuk te beperken.

Bijlage 4: Beveiligingsmaatregelen ter uitwerking van artikel 7

In te vullen door verwerker

Bijlage 5: Omschrijving werkzaamheden ter uitwerking van artikel 8 lid 5
In te vullen door verwerker

Verwerker maakt bij de uitvoering van de verwerkersovereenkomst gebruik van de derden/onderaannemers die in deze bijlage zijn vermeld. De verwerker zal deze bijlage conform artikel 8 van deze verwerkersovereenkomst bijwerken indien er wijzigingen plaatsvinden in de ingeschakelde derden/onderaannemers en deze lijst onverwijld ter beschikking stellen aan de verwerkingsverantwoordelijke.

[PARTIJ 1]	
Vestigingsplaats:	
Inschrijvingsnummer handelsregister:	
Beschrijving van de werkzaamheden:	
Voorwaarden van de verwerkingsverantwoordelijke gesteld aan toestemming:	

[PARTIJ 2]	
Vestigingsplaats:	
Inschrijvingsnummer handelsregister:	
Beschrijving van de werkzaamheden:	
Voorwaarden van de verwerkingsverantwoordelijke gesteld aan toestemming:	

Bijlage 3 van het privacyreglement Slow Food Nederland

Register verwerkingen persoonsgegevens:

Verwerking I

- Persoonsgegevens type A [bijv: bestuur Slow Food Nederland]
- Welke gegevens:
    - Naam
    - Contactgegevens
    - Verjaardagsdatum, leeftijd
    - Bankrekeningnummer
    - Persoon om in voorkomend geval (ziektye, ongeval etc.) te waarschuwen
    - BSN
- Coördinator: [naam]
- Soort verwerking [verzamelen, bewaren, gebruiken voor betalingen, …]
- Verwerker: [naam]
- Bijzondere persoonsgegevens betrokken? Ja/neen. Zo ja, welke?
-

Verwerking II

- Persoonsgegevens type b [bijv: bestuur community]
- Welke gegevens:
    - Naam
    - Contactgegevens
    - bankrekeningnummer
- Coördinator: [naam]
- Soort verwerking [verzamelen, bewaren, gebruiken voor betalingen, …]
- Verwerker: [naam]
- Bijzondere persoonsgegevens betrokken? Ja/neen. Zo ja, welke?

Etc.

Register incidenten

Incident I

1) Datum
2) Omschrijving incident
3) Kwalificatie incident: datalek Ja/neen
4) Betrokken gegevens
5) Betrokkenheid verwerker
6) Betrokkenheid derden
7) Omschrijving risico
8) Melding aan AP ja/neen
9) Melding aan betrokkene ja/neen
10) Afschrift meldingsformulier
11) Omschrijving overige handeling naar aanleiding van het incident
12) Maatregelen ter voorkoming in de toekomst
13) Ondertekening, naam en datum

Incident II

1) Datum
2) Omschrijving incident
3) Kwalificatie incident: datalek Ja/neen
4) Betrokken gegevens
5) Betrokkenheid verwerker
6) Betrokkenheid derden
7) Omschrijving risico
8) Melding aan AP ja/neen
9) Melding aan betrokkene ja/neen
10) Afschrift meldingsformulier
11) Omschrijving overige handeling naar aanleiding van het incident
12) Maatregelen ter voorkoming in de toekomst
13) Ondertekening, naam en datum

etc.

Bijlage 4 van het privacyreglement Slow Food Nederland

Protocol Datalekken

Inleiding

Vanaf 25 mei 2018 zal de meldplicht datalekken uit de Algemene Verordening Gegevensbescherming (“AVG”) de thans bekende bepaling die hierop is gebaseerd uit de Wet bescherming persoonsgegevens (“Wbp”) vervangen. Deze meldplicht houdt in dat organisaties, in het geval van een datalek, dat – onder voorwaarden – moeten melden bij de Autoriteit Persoonsgegevens (‘AP’). Deze melding moet binnen 72 uur na ontdekking zijn gedaan. In bepaalde gevallen moet het datalek ook worden gemeld aan de personen van wie de persoonsgegevens zijn gelekt, de betrokkenen. Indien een datalek niet gemeld wordt kan daarvoor een boete worden opgelegd door de AP.

Dit Protocol Datalekken moet ervoor zorgen dat de juiste mensen op het juiste moment worden geïnformeerd en geactiveerd. Wie moeten intern op de hoogte worden gebracht van een inbreuk? Wie bepaalt of het datalek al dan niet gemeld moet worden? Met welke juridische aspecten dient rekening te worden gehouden?

Meldplicht datalekken van toepassing

In dit hoofdstuk wordt kort uiteengezet wat een datalek is en in welke gevallen sprake is van een wettelijke verplichting om een datalek te melden.

Wat is een datalek?

Een datalek is een inbreuk in verband met persoonsgegevens en wordt door de AVG nader gedefinieerd als 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. Hierbij kan men denken aan bijvoorbeeld het kwijtraken van een USB-stick, de diefstal van een laptop, besmetting met malware of een inbraak door een hacker.
Om te beoordelen of er sprake is van een datalek waarvoor een meldplicht bestaat, moet allereerst worden vastgesteld of gesproken kan worden van een verwerking van persoonsgegevens.

- Persoonsgegevens
  Dit betreft alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (“de betrokkene”). Als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals: een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.

- Verwerking
  Dit is een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens.

De verplichting om een datalek te melden rust op de verwerkingsverantwoordelijke. Dat is ook het geval als het datalek bij de verwerker heeft plaatsgevonden.

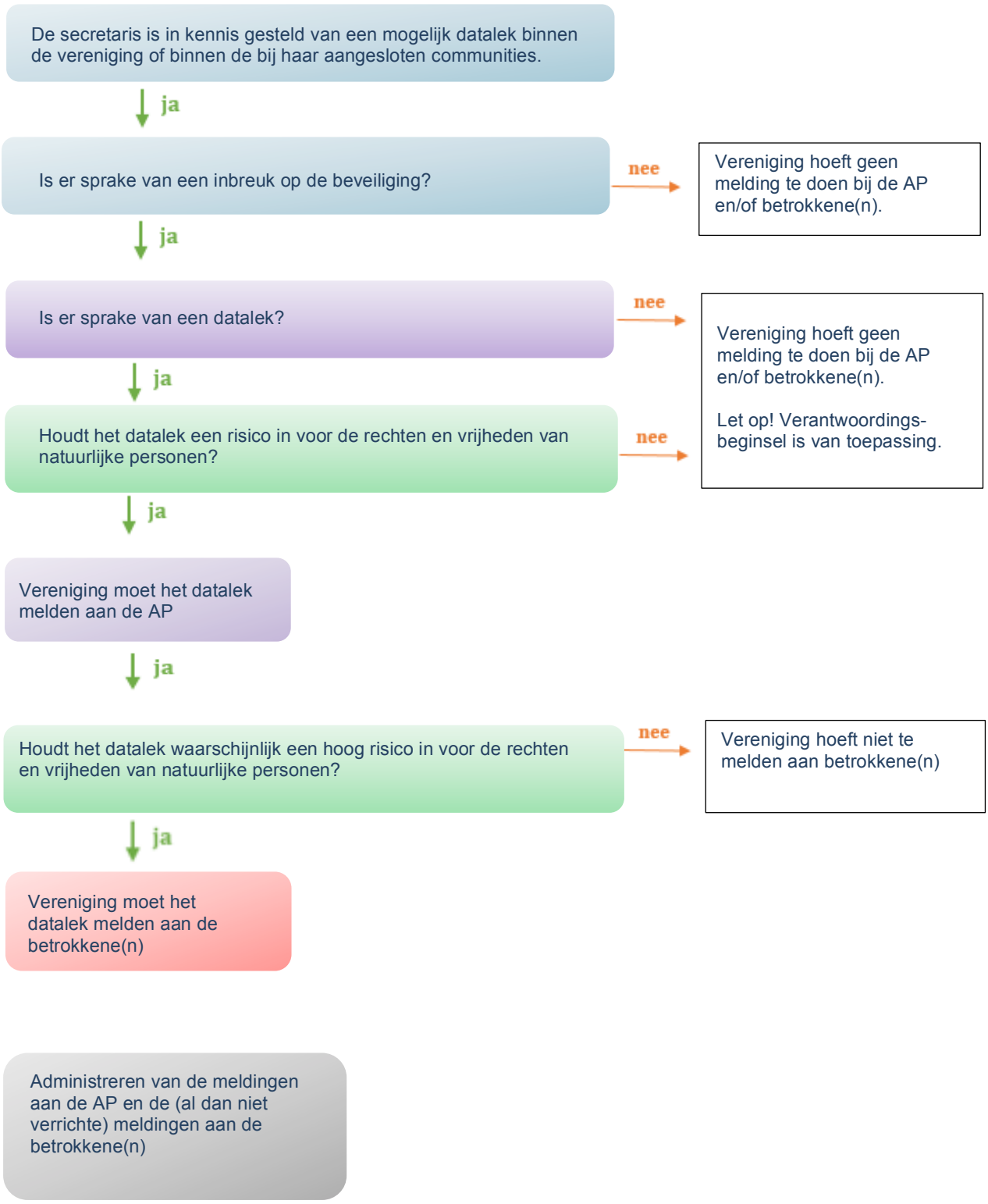
- Verwerkingsverantwoordelijke
  De verwerkingsverantwoordelijke is degene die, alleen of tezamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt. Het gaat hierbij om de vraag wie uiteindelijk bepaalt welke verwerking plaatsvindt van persoonsgegevens voor welk doel.

Bovendien is van belang wie er beslist over op welke manier de gegevensverwerking zal plaatshebben. Deze bevoegdheden kunnen soms in verschillende handen liggen. In dergelijke gevallen is er sprake van gezamenlijke verantwoordelijken. Zij zullen onderling moeten afspreken wie in het voorkomende geval de melding van een datalek moet doen.

- Verwerker
  Een verwerker verwerkt persoonsgegevens ten behoeve van de verwerkingsverantwoordelijke, waarbij doel en middelen door de verwerkingsverantwoordelijke wordt bepaald.

Wanneer een datalek wordt vermoed bij de verwerking van persoonsgegevens, dan zal de secretaris van het bestuur als eindverantwoordelijke voor de handhaving van privacyregels onderstaand schematische beslismodel moeten doorlopen om vast te stellen of het datalek al dan niet gemeld moet worden aan de AP en eventueel aan betrokkenen.

Schematische weergave van het Protocol Datalekken van Vereniging/Stichting



Het is aan te bevelen ieder datalek te evalueren. Zie bijlage 3: Evaluatieformulier

UITWERKING VAN HET PROTOCOL DATALEKKEN

Hieronder volgt een chronologisch overzicht van de verschillende acties die genomen dienen te worden indien een datalek wordt vermoed. De vereniging dient deze te allen tijde te doorlopen bij een mogelijk datalek. Het stappenplan wijst de verantwoordelijken aan en verdeelt de noodzakelijke taken en besluitvorming.

STAP 1: Interne melding wegens een inbreuk op de beveiliging

Een inbreuk op de beveiliging is een gebeurtenis waardoor mogelijk de vertrouwelijkheid, integriteit of beschikbaarheid van informatie in gevaar is, of kan komen. Ieder vermoeden van 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 (persoons)gegevens, behoort volgens onderstaande schema te worden gemeld.

Een medewerker of verwerker van de vereniging raakt bekend met een eventuele inbreuk op de beveiliging in verband met (persoons)gegevens van de vereniging.

Ook een inbreuk op de beveiliging bij een derde partij die persoonsgegevens verwerkt voor de vereniging, een verwerker, kan een meldplicht voor de vereniging tot gevolg hebben. Ieder vermoeden van een inbreuk op de beveiliging behoort direct te worden gemeld aan de secretaris van het bestuur. De verplichting voor een verwerker om een inbreuk op de beveiliging direct te melden volgt uit schriftelijk gemaakte afspraken, zoals bijvoorbeeld uit een verwerkersovereenkomst.

Direct door de medewerker of verwerker uit te voeren acties:
Contact opnemen met de secretaris, in onderstaande volgorde:

- Telefonisch naar de secretaris;
- Vervolgens via secretaris@slowfood.nl middels het Meldingsformulier Beveiligingsinbreuk (**Bijlage 1**).

De medewerker of verwerker dient stand-by te staan voor eventuele (vervolg)vragen uit de organisatie en zal deze in een voorkomend geval met de hoogste prioriteit in behandeling nemen.

Verantwoordelijken STAP 1:

- Medewerker
- Verwerker (indien van toepassing)
- de secretaris van het bestuur

Direct door de secretaris uit te voeren acties:

- Per e-mail een ontvangstbevestiging sturen naar de betreffende persoon die de melding heeft gemaakt (s.v.p. daarin het verzoek opnemen dat deze persoon stand-by dient te zijn en blijven)
- Inwinnen van informatie m.b.t. de inbreuk op de beveiliging en deze vastleggen in het register Incidenten
- Onderzoeken van het (mogelijke) datalek. Is er sprake van een inbreuk op de organisatorische en/of technische beveiligingsmaatregelen van de vereniging (**STAP 2**)

STAP 2: Is er sprake van een datalek?

Niet iedere inbreuk op de beveiliging is ook daadwerkelijk een datalek. Aan de hand van het onderstaande schema zal komen vast te staan of er daadwerkelijk sprake is van een datalek.

De secretaris beoordeelt de gemaakte (interne) melding en beoordeelt of:

1) De inbreuk op de beveiliging tot gevolg heeft dat Vereniging/Stichting niet langer over de (persoons)gegevens beschikt (vernietigd, dan wel op andere wijze verloren gegaan)?

   En

2) Wel/niet redelijkerwijs kan worden uitgesloten dat de inbreuk op de beveiliging heeft geleid tot: (i) wijziging (ii) ongeoorloofde verstrekking van of (iii) ongeoorloofde toegang tot de doorgezonden, opgeslagen of anderszins verwerkte gegevens;

Indien De secretaris tot het oordeel komt dat er:

- **Geen** sprake is van een datalek → dan kan worden overgegaan op sluiting van het dossier (Let op! Het verantwoordingsbeginsel is van toepassing. Dit houdt in dat het oordeel van De secretaris gemotiveerd moet worden geregistreerd en opgeslagen in register Incidenten
- **Wel** sprake is van een datalek → **VERVOLG STAP 3**

Verantwoordelijken STAP 2:

- de secretaris

STAP 3: Meldplicht aan de AP en betrokkene(n)?

Bij STAP 2 is vastgesteld dat er sprake is van een datalek. Niet elk datalek behoeft te worden gemeld aan de AP. Wanneer er wel gemeld moet worden aan de AP, dan betekent dat niet automatisch dat er ook moet worden gemeld aan de betrokkene(n). Aan de hand van het onderstaande schema zal vast komen te staat of, en zo ja aan welke meldingsplicht(en) voldaan dient te worden.

De secretaris beoordeelt eerst of:
Het datalek een risico inhoudt voor de rechten en vrijheden van betrokkene(n)

- Zo ja, dan is er sprake van een meldplicht aan de AP. **VERVOLG STAP 4**.
- Zo nee, dan is er geen sprake van een meldplicht aan de AP. Geen verdere acties vereist. Er kan worden overgegaan tot sluiting van het dossier (Let op! Het verantwoordingsbeginsel is van toepassing. Dit houdt in dat het oordeel van de secretaris gemotiveerd moet worden geregistreerd en opgeslagen in register Incidenten.

Verantwoordelijken STAP 3:
De secretaris

Indien door de secretaris is vastgesteld dat er gemeld moet worden aan de AP, dan zal de secretaris vervolgens moeten oordelen of:
Het datalek waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van betrokkene(n)

- Zo ja, dan zal er – naast de meldplicht aan de AP– ook sprake zijn van een meldplicht aan de betrokkene(n). **VERVOLG STAP 5**.

  NB. De mededeling aan betrokkenen is niet vereist wanneer deze onevenredige inspanning vergt. In dat geval volstaat een openbare mededeling of soortgelijke maatregel waarbij de betrokkenen even doeltreffend worden geïnformeerd.
- Zo nee, dan kan de melding aan de betrokkene(n) achterwege blijven. (Let op! Het verantwoordingsbeginsel is van toepassing. Dit houdt in dat het oordeel van de secretaris gemotiveerd moet worden geregistreerd en opgeslagen in het register Incidenten.

Het IDT komt tot een besluit om wel/geen melding te maken bij de AP en/of betrokkene(n). Dit besluit zal gemotiveerd worden vastgelegd in het register Incidenten.

STAP 4: Melden datalek aan de AP

Indien het datalek gemeld moet worden aan de AP, dan dient dit via onderstaande schema te verlopen.

Het IDT zal de melding aan de AP afwikkelen (binnen 72 uur nadat de datalek is ontdekt).

- Hiertoe dient een door de AP gestandaardiseerd webformulier te worden ingevuld. Deze vragen zijn ook te vinden in **Bijlage 2 Meldingsformulier AP**.

- Zorg ervoor dat allereerst de vragen uit **Bijlage 2** worden ingevoerd omwille van de eigen administratie, alvorens het webformulier van de AP wordt ingevuld. De AP verstrekt namelijk geen afschrift van de melding. Wel geven zij een meldingsnummer. Registreer dit nummer op het Meldingsformulier AP.

De secretaris zal de melding registreren in het register Incidenten.
NB. Indien het onmogelijk is de melding te doen binnen de gestelde termijn van 72 uur, dan zal de AP geïnformeerd moeten worden over de reden hiervan.

Verantwoordelijken STAP 4:

- de secretaris

STAP 5: Melden datalek aan betrokkene(n)

Ingeval het datalek eveneens moet worden gemeld aan de betrokkene(n), dan dient uitvoering te worden gegeven aan het onderstaande schema.

Het IDT zal het volgende bepalen:

- **De wijze van kennisgeving** (bijv.: (i) volledige kennisgeving per e-mail of brief; (ii) summiere kennisgeving per e-mail of brief met verwijzing naar uitgebreidere informatieverstrekking op de website van Vereniging/Stichting; (iii) summiere kennisgeving per e-mail of brief met verwijzing naar centraal informatiepunt; (iv) de media erbij betrekken etc.); en
- **De termijn van kennisgeving** aan de betrokkene(n). Dit moet onverwijld gebeuren. (Deze termijn wordt bovendien vermeld in de melding datalekken aan de AP);
- **Actieplan** wie, wat, waar, wanneer en hoe?

Verantwoordelijken STAP 5:

- secretaris

De secretaris stelt een kennisgeving op.

STAP 6 Bewaarplicht & Administratie

Tot slot geldt voor iedere verrichte melding bij de AP, ongeacht of Vereniging/Stichting ook aan betrokkene(n) heeft gemeld, de onderstaande 3-jarige bewaarplicht.

De gegevens omtrent iedere verrichtte melding van een datalek aan de AP (en eventueel aan de betrokkene(n)), dient 3 jaar te worden bewaard. Eveneens dient het totaaloverzicht te worden bijgehouden en in de digitale kluis bij All United B.V. te worden opgeslagen (**Bijlage 2**).

Verantwoordelijken STAP 6:

- secretaris

Het IDT zal jaarlijks nagaan of de in eerste instantie eventueel achterwege gelaten meldingen aan betrokkenen als gevolg van nieuwe omstandigheden en/of ontwikkelingen nu alsnog dient te worden verricht.

Bijlage 1: Meldingsformulier Beveiligingsinbreuk

Onderstaand meldingsformulier dient u te gebruiken indien zich een inbreuk op de beveiliging heeft voorgedaan. Mogelijk is dit een datalek, waarvoor een wettelijke meldplicht bestaat aan de Autoriteit Persoonsgegevens en eventueel aan de betrokkene(n). Het ingevulde meldingsformulier kunt u sturen naar secretaris@slowfood.nl waarna u een ontvangstbevestiging ontvangt. De secretaris zal beoordelen of er sprake is van een datalek en of deze gemeld moet worden. Bij vragen kunt u telefonisch contact opnemen met de secretaris. Het telefoonnummer wordt iedere verwerker medegedeeld.

ALGEMENE INFORMATIE	
Voor- en achternaam van de melder	
Community/Afdeling	
Telefoonnummer	
E-mailadres	
Datum en tijdstip van ontdekking	
BEVEILIGINGSINBREUK	
Datum en tijdstip	*Van wanneer tot wanneer duurde de inbreuk op de beveiliging?*
Locatie	*Waar heeft de inbreuk op de beveiliging zich voorgedaan?*
Welke gegevens zijn hierbij betrokken?	*Bijvoorbeeld: interne bedrijfsgegevens, medewerkersinformatie; gegevens sollicitanten; klantinformatie; of anders?*
Korte omschrijving van de inbreuk op de beveiliging en hoe dit is ontdekt:	
Waarop heeft de beveiligingsinbreuk betrekking?	*Bijvoorbeeld:* *Papieren documenten: brieven, externe documenten, kopieën;* *Digitale informatie: informatiesysteem, bestand, e-mail;* *Apparaat: desktop, laptop, tablet, smartphone, harde schijf;* *Media: externe harde schijf, USB-stick;*
Is bekend of het apparaat c.q. de informatie met een wachtwoord is beschermd?	
Is bekend of het apparaat c.q. de informatie is versleuteld?	

Is bekend of er identificerende gegevens zijn gelekt?	*Bijvoorbeeld: burgerservicenummer, klantinformatie, of gebruikersnamen en wachtwoorden*
Is bekend om hoeveel records het kan gaan?	*Zo ja, hoeveel (bij benadering)?*
Is de beveiligingsinbreuk al gestopt?	*Zo ja, hoe en wanneer?*
Wie of welke partijen zijn er nog meer reeds op de hoogte van de beveiligingsinbreuk?	
Overige informatie	

Bedankt voor het maken van de melding! Voor eventuele (vervolg)vragen verzoeken wij u stand-by te blijven en in voorkomend geval deze met de hoogste prioriteit in behandeling te nemen.

Bijlage 2: Meldingsformulier AP

Onderstaande vragen worden gesteld door de AP wanneer Vereniging/Stichting melding doet van een datalek. Belangrijk is dat deze eerst voor eigen administratie beantwoord en opgeslagen worden in de digitale kluis bij All United B.V., alvorens de daadwerkelijke melding bij de AP wordt gemaakt via het webformulier. Dit is nodig omdat de AP geen afschrift geeft van de gemaakte melding. Echter moet Vereniging/Stichting hier wel over (blijven) beschikken, omdat er een documentatieplicht bestaat. Wel geeft de AP een meldingsnummers. Noteer deze op het meldingsformulier hieronder.

Nieuwe of bestaande melding		
Gaat het om een nieuwe of bestaande melding?	Nieuwe melding	Bestaande melding

Wettelijk kader van de melding			
Op grond van welke wettelijke bepaling doet u deze melding?	Wet Bescherming Persoonsgegevens, artikel 34a, eerste lid.	Telecommunicatiewet, artikel 11.3a, eerste lid.	Algemene Verordening Gegevensbescherming, artikel 33 lid, eerste lid.

Algemene informatie en contact persoon		
Over welke organisatie of welk bedrijf gaat het?	Naam van het bedrijf of de organisatie	
	Adres (bezoekadres)	
	Postcode	
	Vestigingsplaats	
	Registratienummer bij de Kamer van Koophandel	
Wie meldt het datalek?	Naam	
	Functie	
	E-mailadres	
	Telefoonnummer	
	Tweede telefoonnummer	

Met wie kan de Autoriteit Persoonsgegevens contact opnemen voor nadere informatie over de melding?		
De melder is contactpersoon	Ja	Nee
	Naam contactpersoon	
	Functie contactpersoon	
	E-mailadres contactpersoon	
	Telefoonnummer contactpersoon	
	Tweede telefoonnummer contactpersoon	
In welke sector is de organisatie of het bedrijf actief?	Handel en dienstverlening	
	Openbaar bestuur	
	Overige sector, te weten: Politie en justitie	
	Sociale Zekerheid	
	Telecom	
	Zorg en welzijn	
	Overige sector, te weten:	

Gegevens over het datalek		
Geef een samenvatting van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest		
Vond de inbreuk plaats in een verwerking die is uitbesteed aan een andere organisatie?	Ja	Nee
	Naam van de organisatie waaraan de verwerking is uitbesteed	
	Van minimaal hoeveel personen zijn persoonsgegevens betrokken bij de inbreuk?	
	Van maximaal hoeveel personen zijn persoonsgegevens betrokken bij de inbreuk?	
	Omschrijf de groep mensen van wie persoonsgegevens zijn betrokken bij de inbreuk.	
Is bekend wanneer de inbreuk was?	Ja	Nee
Is de exacte datum bekend wanneer de inbreuk was?	Ja	Nee
	Exacte datum waarop de inbreuk was	
	Start datum van de periode waarbinnen de inbreuk was	
	Eind datum van de periode waarbinnen de inbreuk was	
	Wanneer werd de inbreuk ontdekt?	

Wat is de aard van de inbreuk? **Selecteer één of meerdere opties**		
Lezen (vertrouwelijkheid)	Ja	Nee
Kopiëren	Ja	Nee
Veranderen (integriteit)	Ja	Nee
Verwijderen of vernietigen (beschikbaarheid)	Ja	Nee
Diefstal	Ja	Nee

Nog niet bekend	Ja	Nee

Om welk type persoonsgegevens gaat het? **Selecteer één of meerdere opties en geef, indien van toepassing, een toelichting**		
Naam-, adres- en woonplaatsgegevens	Ja	Nee
Telefoonnummers	Ja	Nee
E-mailadressen of andere adressen voor elektronische communicatie	Ja	Nee
Toegangs- of identificatiegegevens	Ja	Nee
Financiële gegevens	Ja	Nee
Burgerservicenummer (BSN)	Ja	Nee
Paspoortkopieën of kopieën van andere legitimatiebewijzen	Ja	Nee
Geslacht, geboortedatum en/of leeftijd	Ja	Nee
Bijzondere persoonsgegevens	Ja	Nee
Overige / onbekend		

Welke gevolgen kan de inbreuk hebben voor de persoonlijke levenssfeer van de betrokkenen? **Selecteer één of meerdere opties**		
Stigmatisering of uitsluiting	Ja	Nee
Schade aan de gezondheid	Ja	Nee
Blootstelling aan (identiteits)fraude	Ja	Nee
Blootstelling aan spam of phishing	Ja	Nee
Andere gevolgen, namelijk:	Ja	Nee

Vervolgacties naar aanleiding van het datalek	
Welke technische en	

organisatorische maatregelen heeft uw organisatie getroffen om de inbreuk aan te pakken en om verdere inbreuken te voorkomen?			
Heeft u het datalek gemeld aan de betrokkenen of bent u van plan dat te gaan doen?	Ja	Nee	Nog niet bekend
Wanneer heeft u het datalek gemeld aan de betrokkenen?			
Wanneer gaat u het datalek melden aan de betrokkenen?			
Wat is de inhoud van de melding aan de betrokkenen?			
Hoeveel betrokkenen heeft u geïnformeerd of gaat u informeren?			
Welk communicatiemiddel of welke communicatiemiddelen gebruikt u of gaat u gebruiken om de betrokkenen te informeren?			

Waarom ziet u af van het melden van het datalek aan de betrokkenen?	
De technische beschermingsmaatregelen die ik heb getroffen bieden voldoende bescherming om de melding aan de betrokkene achterwege te kunnen laten	
Het is onwaarschijnlijk dat het datalek ongunstige gevolgen zal hebben voor de persoonlijke levenssfeer van de betrokkenen, want:	
Ik heb zwaarwegende	

redenen om de melding aan de betrokkene achterwege te laten, namelijk:	
Anders, namelijk:	

Technische beschermingsmaatregelen		
Waren de persoonsgegevens op het moment van het ontdekken van het datalek versleuteld, gehasht of op een andere manier onbegrijpelijk of ontoegankelijk voor onbevoegden?	Deels, namelijk:	
	Ja	Nee
Als de persoonsgegevens geheel of deels onbegrijpelijk of ontoegankelijk waren gemaakt, op welke manier is dit dan gebeurd?		

Internationale aspecten		
Heeft de inbreuk betrekking op personen in andere EU-landen?		
Nee	Nog niet bekend	
Ja, namelijk:		
Heeft uw organisatie, of bedrijf, het datalek gemeld bij toezichthouders in een of meer andere EU-landen, of gaat u dat nog doen?	Ja	Nee
Toezichthouder(s) van andere landen waar het datalek is gemeld		

Vervolgmelding

Is naar uw mening deze melding compleet?	Ja, de vereiste informatie is verstrekt en er is geen vervolgmelding nodig	
	Nee, er komt later een vervolgmelding met aanvullende informatie over deze inbreuk	
Door dit vakje aan te vinken verklaart u bevoegd te zijn deze melding te doen en dat de in de melding verstrekte informatie juist is.		

Bijlage 3: Evaluatieformulier

Ieder datalek moet worden geëvalueerd om zodoende lering te trekken uit de stappen en beslissingen die zijn genomen gedurende het proces van de incidentafhandeling. Belangrijk is om onderscheid te maken in het type datalek, omdat kleine incidenten met beperkte impact routinematig kunnen worden afgehandeld en daarom ook op deze manier kunnen worden geëvalueerd. Daarnaast zijn er bijzondere datalekken met grote impact. Dergelijke datalekken dienen altijd individueel geëvalueerd te worden om te beoordelen of dit incident aanleiding geeft om procedures voor het voorkomen of afhandelen van datalekken te optimaliseren.

Wat was de oorzaak van het datalek, en welke maatregelen zijn genomen om herhaling te voorkomen?
Hoe is het incident ontdekt, en zijn daarin verbeteringen nodig?
Hoe is het incident intern beoordeeld, en zijn daarin verbeteringen nodig?
Hoe is het incident bestreden, en wat kon daar beter?
Hoe functioneerde het Interne Datalek Team?
Wat was de kwaliteit van het bepalen van de impact, en kon dit sneller of beter?
Hoe verliep de meldaanpak (naar de Autoriteit Persoonsgegevens en betrokkene(n)? Wat kon beter?

Hoe verliep de herstelaanpak, en wat kon beter?
Verbetering informatiebeveiliging; *Nazorg aan betrokkenen: contactpunt, voorlichting, ondersteuning.* *Organisatiebelang: juridische ondersteuning, reputatie, klantvertrouwen, schadeafhandeling etc.*
Indien bekend is hoe de AP het datalek heeft beoordeeld, wat zijn dan onze lessen?
Is bekend hoe de betrokkene(n) de melding en nazorg hebben ervaren? Zo ja, hoe?
Is bekend hoe andere partijen (belanghebbenden) het datalek, onze communicatie daarover en het en de afhandeling ervan beoordelen? Had dit beter gekund? Zo ja, hoe dan?