**Protocol voor inbreuken in verband met persoonsgegevens**

In dit document vindt u het protocol wanneer een datalek plaatsvindt binnen Maizena en welke stappen Maizena moet ondernemen. Het is sinds 25 mei 2018 door de Algemene Verordening Gegevensbescherming verplicht om datalekken te melden. Deze meldplicht geldt zowel voor de betrokkene(n) als bij de Radboud Universiteit te Nijmegen.

De studievereniging heeft de bevoegdheid om per inbreuk in verband met persoonsgegevens te bepalen of de procedure volledig gevolgd moet worden of dat hiervan afgeweken kan worden. Het doel van deze procedure is om vast te leggen welke stappen genomen moeten worden door Maizena bij het vermoeden van of het kennisnemen van een incident dat (mogelijk) aangemerkt kan worden als een inbreuk in verband met persoonsgegevens. Hiermee wordt het volgende resultaat nagestreefd:

* Het steeds volgen van een eenduidige procedure.
* Het zorgvuldig waarborgen van belangen van de studievereniging, het individu dan wel een andere organisatie die betrokken is bij het incident, zijnde een (mogelijke) inbreuk in verband met persoonsgegevens.
* Het op zorgvuldige en systematische wijze analyseren van een incident, zijnde mogelijk datalek, zodat aanwezige risicomomenten in het proces zichtbaar worden. Centraal staat hierbij het vaststellen van de onvolkomenheden in de (toepassing van) technische en organisatorische beveiligingsmaatregelen, die (mogelijk) hebben kunnen leiden tot het incident.
* Het aanwijzen van een bestuursverantwoordelijke omtrent inbreuken in verband met persoonsgegevens en het aanwijzen van een instantie waarbij aangeklopt kan worden bij het ontdekken van een (mogelijke) inbreuk. Daarbij kan gedacht worden aan een privacycoördinator van de Radboud Universiteit. In het geval van Maizena is dat het FG-Bureau van de Radboud Universiteit.

**Aanpak inbreuk in verband met persoonsgegevens**

Wanneer er dus sprake is van een (mogelijke) inbreuk in verband met persoonsgegevens dan kan het volgende processchema aangehouden worden. Na het schema zal een uitleg per stap beschreven worden.



\* Datalek refereert hier naar inbreuk in verband met persoonsgegevens

**1. Identificeren mogelijke inbreuk in verband met persoonsgegevens**

Indien een (mogelijke) inbreuk in verband met persoonsgegevens wordt geconstateerd, wordt de rest van het bestuur ingelicht. De bestuursverantwoordelijke voor inbreuken in verband met persoonsgegevens bepaalt daarbij of hij/zij het probleem alleen op zich neemt of een ander bestuurslid (of eventueel een oud-bestuurder/actief lid) betrekt in het proces.

**2. Bestuursverantwoordelijke; beoordelen aard/ernst incident & verslag brengen aan rest van het bestuur**

De bestuursverantwoordelijke (en eventuele andere hulp) onderzoeken de inbreuk in verband met persoonsgegevens om te zien of er daadwerkelijk sprake is van een inbreuk. Als het een inbreuk in verband met persoonsgegevens betreft, wordt er gekeken naar de informatie die gelekt is en de ernst van de inbreuk. De bestuursverantwoordelijke rapporteert de uitslag aan de rest van het bestuur. Bij de beoordeling spelen de volgende punten een rol:

* Is er sprake van verlies van persoonsgegevens? Dit houdt in dat de studievereniging deze gegevens niet meer heeft, omdat deze zijn vernietigd of op een andere wijze verloren zijn gegaan;
* Is er sprake van onrechtmatige verwerking van persoonsgegevens? Hieronder vallen de onbedoelde of onwettige vernietiging, verlies of wijziging van verwerkte persoonsgegevens, of een niet geautoriseerde toegang tot verwerkte persoonsgegevens of verstrekking daarvan;
* Is er sprake van een enkele tekortkoming van kwetsbaarheid in de beveiliging?
* Kan er redelijkerwijs worden uitgesloten dat een inbreuk op de beveiliging tot een onrechtmatige verwerking heeft geleid?
* Zijn er persoonsgegevens van gevoelige aard gelekt?
	+ Bijzondere persoonsgegevens conform artikel artikel 9 AVG;
	+ Gegevens over de financiële of economische situatie van de betrokkene;
	+ Gegevens die kunnen leiden tot stigmatisering of uitsluiting van de betrokkene;
	+ Gebruikersnamen, wachtwoorden en andere inloggegevens;
	+ Gegevens die kunnen worden gebruikt voor (identiteits)faude.
* Leiden de aard en de omvang van de inbreuk tot (een aanzienlijke kans op) ernstige nadelige gevolgen? Betrek hierbij factoren als:
	+ De omvang van de verwerking; gaat het om veel persoonsgegevens per persoon, en om gegevens van grote groepen betrokkenen?
	+ De impact van verlies of onrechtmatige verwerking;
	+ Het delen van de persoonsgegevens binnen ketens; dit betekent dat de gevolgen van verlies en onbevoegde wijziging van persoonsgegevens door de hele keten kunnen optreden;
	+ Betrokkenheid van kwetsbare groepen; denk aan verstandelijk gehandicapten.

**3. Indien datalek; inlichten aangewezenen instantie en onderzoek naar de inbreuk in verband met persoonsgegevens**

De aangewezen instantie van de Radboud Universiteit wordt op de hoogte gesteld waarmee op basis daarvan plannen worden gemaakt. Daarbij wordt onderzocht hoe de inbreuk in verband met persoonsgegevenszich heeft kunnen voordoen indien dit nog niet bekend was. De aangewezen instantie is CERT-RU, te bereiken op 024-36 2 22 22 (ICT Helpdesk). Buiten kantoortijden is de CERT-RU te bereiken op 024 361 08 18.

**4. Vaststellen inbreuk in verband met persoonsgegevens**

Na overleg met de ICT-helpdesk/ CERT-RU van de Radboud Universiteit, wordt het onderzoek naar de inbreuk in verband met persoonsgegevens afgerond en denkt het gehele bestuur na over vervolgplannen omtrent dit incident.

**5. Rapporteren aan betrokkene(n)**

Het bestuur neemt de afweging of betrokkene(n) ingelicht moeten worden over de inbreuk in verband met persoonsgegevens. Indien dit het geval is, neemt de bestuursverantwoordelijke contact met hen op. Op grond van artikel 34 lid 1 AVG moet een betrokkene geïnformeerd worden wanneer de inbreuk in verband met persoonsgegevens waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen. De mededeling aan de betrokkene omvat in ieder geval een omschrijving, in duidelijke en eenvoudige taal, van de aard van de inbreuk in verband met persoonsgegevens en de in artikel 33 lid 3 AVG genoemde gegevens. Een betrokkene hoeft niet geïnformeerd te worden wanneer een van de volgende voorwaarden is vervuld:

* De verwerkingsverantwoordelijke heeft passende technische en organisatorische beschermingsmaatregelen genomen en deze maatregelen zijn toegepast op de persoonsgegevens waarop de inbreuk in verband met persoonsgegevens betrekking heeft, met name die welke de persoonsgegevens onbegrijpelijk maken voor onbevoegden, zoals versleuteling (artikel 34 lid 3 sub a AVG);
* De verwerkingsverantwoordelijke heeft achteraf maatregelen genomen om ervoor te zorgen dat het in lid 1 bedoelde hoge risico voor de rechten en vrijheden van berokkenen zich waarschijnlijk niet meer zal voordoen (artikel 34 lid 3 sub b AVG);
* De mededeling zou onevenredige inspanningen vergen. In dat geval komt er in de plaats daarvan een openbare mededeling of een soortgelijke maatregel waarbij betrokkenen even doeltreffend worden geïnformeerd (artikel 34 lid 3 sub c AVG).

**6. Verbeteringsmaatregelen bedenken en implementeren**

Naar aanleiding van de inbreuk in verband met persoonsgegevens stelt het bestuur verbeteringsmaatregelen op om een soortgelijke situatie te voorkomen. Deze worden dan ook zo spoedig mogelijk ingevoerd, waarbij ook alle andere mogelijke inbreuken in verband met persoonsgegevens worden onderzocht en verholpen.

**7. Einde**

Daarmee wordt het proces rondom inbreuken in verband met persoonsgegevens afgesloten. Indien er weer een (mogelijke) inbreuk in verband met persoonsgegevenszich voordoet, dan wordt het proces opnieuw in gang gezet.