ALGEMENE VERORDENING GEGEVENSBESCHERMING

Het RijnlandSchouderNetwerk (RSN) is een vereniging. Ten behoeve van het goed functioneren wordt een administratie bijgehouden, waarin alle benodigde informatie wordt geregistreerd.

Welke persoonsgegevens worden geregistreerd?

- NAW-gegevens van de leden, alsmede het werkadres en daarbij horende contactgegevens.

Met welk doel worden deze persoonsgegevens geregistreerd?

- Het onderling kunnen communiceren binnen de vereniging
- Het versturen van facturen met betrekking tot lidmaatschap
- Het kunnen aanvragen van accreditatiepunten bij het KNGF

Wie is verantwoordelijk voor het op een juiste manier registreren van de persoonsgegevens?

- de secretaris van het RSN

Wie heeft er toegang tot deze gegevens?

- het gehele bestuur heeft toegang tot de ledenadministratie, om reden dat bij uitval van de secretaris een ander bestuurslid zijn/haar taken kan waarnemen.

Welke maatregelen worden genomen om te voorkomen dat onbevoegden toegang krijgen tot deze gegevens?

Ieder persoon die toegang heeft tot de deze gegevens is er verantwoordelijk voor....

- het up-to-date houden software en besturingsprogramma op ieder apparaat waarmee toegang tot de gegevens kan worden verkregen.

- de aanwezigheid van de meest recente virusscanner op ieder apparaat waarmee toegang tot de gegevens kan worden verkregen
- beveiligde internetverbinding. In geval van WiFi dient er een wachtwoord te zijn ingesteld.

Algemeen: de website is beveiligd middels een ssl-certificaat.

Wat te doen in geval van (digitale) inbraak?

- alle datalekken worden gedocumenteerd.
- in geval van een ernstig datalek wordt er direct melding gedaan bij Autoriteit Persoonsgegevens. (zie onderstaand toelichtende tekst)
- zo nodig zullen betrokkenen geïnformeerd worden. (zie onderstaand toelichtende tekst)

Toelichting

De meldplicht datalekken houdt in dat organisaties direct melding moeten doen bij de Autoriteit Persoonsgegevens in geval van een ernstig datalek. De Autoriteit Persoonsgegevens heeft beleidsregels meldplicht datalekken opgesteld. Deze beleidsregels zijn bedoeld om organisaties te helpen bij het bepalen of er sprake is van een datalek dat zij moeten melden bij de Autoriteit Persoonsgegevens en eventueel aan de betrokkenen. De AVG stelt strengere eisen aan uw eigen registratie van de datalekken die zich in uw organisatie hebben voorgedaan. U moet ALLE datalekken documenteren. Met deze documentatie moet de AP kunnen controleren of u aan de meldplicht heeft voldaan. Bron: www.autoriteitpersoonsgegevens.nl.

Risico-analyse

- de kans op een (digitale) inbraak is klein, gezien bovenstaande maatregelen in combinatie met het feit dat we een kleine vereniging zijn en daarom minder interessant voor hackers.
- bij een eventuele (digitale) inbraak zal de impact zeer klein zijn.