Toegang

De toegang tot de persoonsgegevens is beperkt tot de personen die toegang hebben tot Sportlink middels een gebruikersaccount met eigen wachtwoord. De toegangsrechten tot de persoonsgegevens zijn beperkt tot wat iemand nodig heeft voor het uitoefenen van zijn of haar functie binnen de voetbalvereniging. De toegangsrechten worden aangepast bij een functiewissel en ingetrokken wanneer een persoon stopt met de functie. De ledenadministratie wordt uitgevoerd door de secretaris. De secretaris is in principe de enige persoon die persoonsgegevens mag invoeren, wijzigen en verwijderen. Er wordt aan één ander bestuurslid de toegangsrechten verleend, zodat deze bij uitzonderlijke situaties de taak kan overnemen.

Verenigingswifi

De verenigingswifi is alleen beschikbaar voor bestuur en commissieleden. Bij hoge uitzondering kan een KNVB-scheidsrechter toegang krijgen tot de verenigingswifi in verband met het invullen van de wedstrijdzakenapp. Het wachtwoord is enkel bekend bij bevoegde personen. Het wachtwoord wordt niet gedeeld met leden of gasten. Er is geen ‘gast-wifi’ binnen onze vereniging.

Beveiliging apparaten

De computers, laptops, telefoons en USB-sticks waarop persoonsgegevens worden verwerkt zijn beveiligd met een adequaat wachtwoord of andere mogelijkheid tot beveiliging.

Wachtwoorden

De wachtwoorden worden niet opgeschreven en worden niet gedeeld. De wachtwoorden worden niet automatisch opgeslagen. Iedereen verandert het wachtwoord minimaal één keer per jaar. Er worden geen wachtwoorden gebruikt die eenvoudig zijn te raden. Een sterk wachtwoord bestaat uit minimaal 8 tekens, waarvan, 1 hoofdletter, een kleine letter, een cijfer en een speciaal teken.

Gebruik applicatie van derden

Sportlink maakt vanwege de zeer gevoelige data gebruik van meervoudige authenticatie. Naast gebruikersnaam en wachtwoord moet er ook een code worden ingevoerd.

Gebruik van privéapparatuur

De vrijwilligers werken doorgaans op privéapparatuur (mobiele telefoons, laptops, desktopcomputers, USB-sticks). De vrijwilligers zorgen ervoor dat het besturingsprogramma, de gebruikte software en antivirussoftware volledig is geüpdatet. Enkel de noodzakelijke persoonsgegevens worden op privéapparatuur opgeslagen. Inkomende e-mails worden automatisch gecontroleerd op virussen, trojans en andere malware.

E-mail

Bij het versturen van e-mailberichten naar meerdere personen wordt zoveel mogelijk gebruik gemaakt van de BCC-regel. Hierdoor zijn de e-mailadressen niet voor iedereen zichtbaar.

Digitale opslag en papieren opslag

Persoonsgegevens worden beveiligd opgeslagen (lokale mappen, e-mails en andere plaatsen). Gebruik beveiliging op mappen en/of bestanden met persoonsgegevens. Bijzondere en gevoelige persoonsgegevens worden alleen gebruikt indien dit van belang is voor het doel. De persoonsgegevens worden zo spoedig mogelijk verwijderd en daarbij wordt ook de prullenbak regelmatig geleegd.

De papieren versies van persoonsgegevens worden adequaat vernietigd (bijvoorbeeld met een papierversnipperaar). Lijsten met deelnemersgegevens worden indien nodig beveiligd verstuurd. In Excel en Word kan je eenvoudig een bestand met een wachtwoord beveiligen. Het versturen van gevoelige of bijzondere persoonsgegevens wordt zo veel mogelijk vermeden.

Kennis en bewustwording

De vrijwilligers die omgaan met persoonsgegevens hebben de kennis hoe ze adequaat moeten omgaan met persoonsgegevens. De vrijwilligers zich bewust van de risico’s.

Jaarlijkse evaluatie/controle

Het bestuur bekijkt ieder jaar de effectiviteit van het beleid, de maatregelen en de beveiliging. De beveiligingsmaatregelen blijven up-to-date en waar nodig worden verbeteringen doorgevoerd.