Digitalisering en privacy: wie krijgt toegang tot welke gegevens?

Websiteartikel | Digitalisering NPO | Week 44 – oktober 2026

De NPO werkt aan de verdere digitalisering van de duivensport. Daarbij speelt NPO Cloud een belangrijke rol. Het doel is om gegevens betrouwbaarder te registreren en veilig beschikbaar te maken voor de werkzaamheden waarvoor ze nodig zijn.

Dat roept ook vragen op. Welke gegevens worden geregistreerd? Wie kan deze bekijken? En hoe voorkomen we dat informatie bij de verkeerde personen terechtkomt?

Privacy en informatiebeveiliging zijn daarom belangrijke voorwaarden bij de verdere ontwikkeling van NPO Cloud.

Waarom worden gegevens digitaal bij elkaar gebracht?

Binnen de duivensport worden gegevens op verschillende plaatsen geregistreerd en gebruikt. Denk aan ledenadministraties, ringnummers, vaccinatiegegevens en informatie over wedstrijddeelname. Wanneer dezelfde gegevens op meerdere plaatsen opnieuw moeten worden ingevoerd, ontstaat extra administratief werk. Bovendien neemt de kans op fouten en verschillen tussen registraties toe. Een belangrijk uitgangspunt van NPO Cloud is daarom: gegevens één keer betrouwbaar registreren en daarna veilig gebruiken waar ze nodig zijn. Dat betekent niet dat iedereen toegang krijgt tot alle informatie. Het betekent dat gegevens op een gecontroleerde manier beschikbaar moeten zijn voor de juiste werkzaamheden.

Wie mag welke gegevens bekijken?

Niet iedere gebruiker heeft dezelfde informatie nodig. Een liefhebber moet bijvoorbeeld zijn eigen gegevens kunnen registreren en bekijken. Een vereniging heeft bepaalde gegevens nodig voor de ledenadministratie en de organisatie van wedvluchten. Afdelingen en de NPO hebben op hun beurt informatie nodig voor hun eigen verantwoordelijkheden en controles.

Het uitgangspunt is daarom dat toegang wordt gekoppeld aan de werkzaamheden en verantwoordelijkheden van de gebruiker. Daarbij moet worden bepaald:

- welke gegevens iemand nodig heeft;
- voor welk doel deze gegevens gebruikt mogen worden;
- welke handelingen iemand mag uitvoeren;
- hoe toegang wordt verleend en beheerd;
- hoe wordt voorkomen dat onbevoegden informatie kunnen inzien of wijzigen.

De verdere inrichting van deze toegangsrechten en bijbehorende afspraken is onderdeel van de uitwerking van de digitaliseringsstrategie.

Een praktijkvoorbeeld: Mijn te enten duiven

In ons vorige artikel beschreven we de pilot ‘Mijn te enten duiven’ in Afdeling Noord. Met deze toepassing kan een liefhebber zelfstandig een entformulier samenstellen, na vaccinatie laten ondertekenen en

vervolgens digitaal uploaden. Het geüploade formulier kan daarna worden ingezien en gecontroleerd door de Vereniging, Afdeling en NPO.

Dit is een concreet voorbeeld van het principe dat gegevens niet telkens opnieuw hoeven te worden aangeleverd. Tegelijkertijd laat het zien waarom duidelijke afspraken over toegang belangrijk zijn. De verschillende betrokken partijen moeten de informatie kunnen gebruiken voor hun eigen taken, zonder dat gegevens onnodig breed beschikbaar worden gemaakt.

Wat betekent dit voor de beveiliging?

Wanneer gegevens digitaal beschikbaar zijn, moeten deze zorgvuldig worden beschermd. Daarom zijn informatiebeveiliging en privacy belangrijke onderdelen van de verdere ontwikkeling. Er moet onder andere aandacht zijn voor het voorkomen van onbevoegde toegang, het zorgvuldig beheren van gebruikersrechten, de betrouwbaarheid van gegevens en afspraken met partijen die systemen ontwikkelen of gegevens verwerken. Ook moet duidelijk zijn wie waarvoor verantwoordelijk is.

De NPO werkt deze technische, organisatorische en juridische afspraken verder uit. Het zou daarom te vroeg zijn om te stellen dat alle maatregelen en overeenkomsten al definitief zijn vastgesteld.

Wat verandert er voor verenigingen?

Verenigingen blijven een belangrijke rol vervullen binnen de duivensport. Digitalisering moet ervoor zorgen dat zij de gegevens die nodig zijn voor hun werkzaamheden eenvoudiger en betrouwbaarder kunnen gebruiken.

Het doel is niet om vrijwilligers met extra administratie te belasten, maar juist om dubbele invoer en onnodige handmatige controles waar mogelijk te verminderen. Dat vraagt wel om een duidelijke inrichting van rollen en toegangsrechten. Welke gegevens een verenigingsfunctionaris kan bekijken of aanpassen, moet passen bij de werkzaamheden die deze persoon uitvoert. De precieze inrichting hiervan wordt verder uitgewerkt.

Wat staat vast en wat wordt nog uitgewerkt?

Dit staat vast

- Privacy en informatiebeveiliging zijn belangrijke uitgangspunten van de digitaliseringsstrategie.
- NPO Cloud moet relevante gegevens veilig en betrouwbaar beschikbaar maken.
- Gegevens moeten alleen worden gebruikt voor de werkzaamheden waarvoor ze nodig zijn.
- Duidelijke afspraken over toegang, verantwoordelijkheden en gegevensgebruik zijn noodzakelijk.

Dit wordt verder uitgewerkt

- De precieze inrichting van gebruikersrollen en toegangsrechten.
- De technische en organisatorische beveiligingsmaatregelen.
- De afspraken met leveranciers en andere betrokken partijen.
- De verdere inrichting van digitale controles en gegevensuitwisseling.

Dit is nog niet definitief vastgesteld

- De volledige inrichting van alle toekomstige gebruikersrechten.
- Alle technische en organisatorische maatregelen voor toekomstige toepassingen.
- De exacte werkwijze voor iedere toekomstige digitale toepassing.

Zorgvuldig omgaan met gegevens

Digitalisering biedt mogelijkheden om de wedstrijdorganisatie eenvoudiger, betrouwbaarder en toekomstbestendiger te maken. Maar dat kan alleen wanneer liefhebbers en verenigingen erop kunnen vertrouwen dat zorgvuldig met hun gegevens wordt omgegaan.

Daarom kijken we bij de ontwikkeling van NPO Cloud niet alleen naar wat technisch mogelijk is, maar ook naar wat noodzakelijk, veilig en verantwoord is. Niet iedereen hoeft alles te kunnen zien. De juiste gegevens moeten beschikbaar zijn voor de juiste personen, voor de juiste werkzaamheden.