	Koninklijke Atletiekclub A.S. RIEME vzw			
	Het PRIVACY beleidsplan			
	RL: **69**	Datum uitgave :	**15 maart 2018**	Versie: **1**

Deze richtlijn is gebaseerd op de informatie van Scwitch en T&C Blue Horizon.

1 Wat is de Algemene Verordening Gegevensbescherming?

1) Het recht op privacy kun je eenvoudig omschrijven als '***iemands recht om met rust gelaten te worden***'. Dit betekent o.a. dat je niet zomaar iemands **persoonlijke informatie** mag gebruiken. Dit laatste noemen we het recht op **de bescherming van persoonsgegevens**.
2) De Algemene Verordening Gegevensbescherming (AVG, of GDPR: General Data Protection Regulation) is een geheel van Europese regels om de burger te beschermen rond gebruik van persoonsgegevens.
3) De GDPR is in werking sinds 24 mei 2016. Ze is van toepassing vanaf 25 mei 2018. Vanaf 25 mei 2018 moet je bij een controle of betwisting actief kunnen aantonen dat je volgens de nieuwe wetgeving handelt.
4) Elke organisatie, ook vzw's en feitelijke verenigingen die persoonsgegevens gebruiken, opslaan of verwerken, vallen onder de regelgeving en moeten zich in orde stellen.
   a) De regelgeving is niet van toepassing als je gegevens uitsluitend gebruikt voor persoonlijk of huiselijk gebruik.
   b) De regelgeving is niet van toepassing als je de persoonsgegevens alleen maar afleest van een papieren drager en die drager nadien niet bijhoudt maar weggooit, vernietigt of teruggeeft aan de eigenaar.

1.1 Wat is de doelstelling van de Verordening

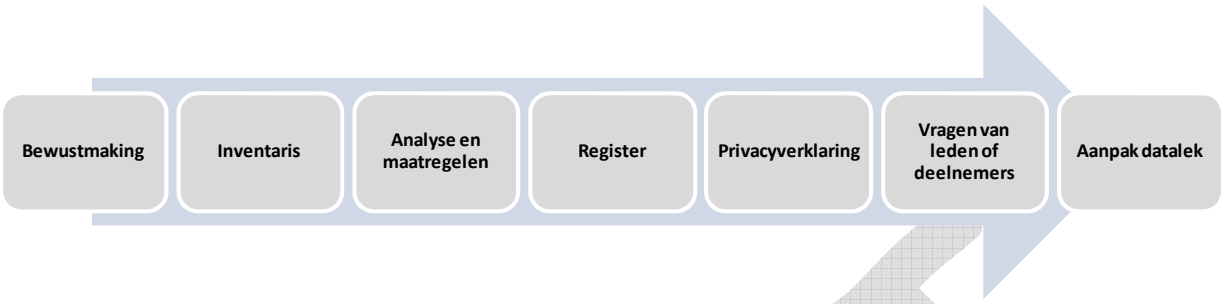
1) Een grotere verantwoordingsplicht, dus meer transparantie over de verwerking, het beheer, de bewaring en eventueel kwijtraken (datalek) van persoonsgegevens.
2) Nadruk op de rechten van de betrokkene.
3) Bewijslast bij de verwerkingsverantwoordelijke en de verwerker.
4) Een sterker toezicht. De Privacycommissie wordt naast informatieorgaan ook waakhond en kan boetes opleggen.

1.2 Wanneer is onze club in regel met de Verordening?

1) We hebben privacy en GDPR **besproken** op ons bestuur, vrijwilligersvergadering(en) …
2) Binnen onze club is er iemand **verantwoordelijk/aanspreekpunt** rond GDPR.
3) Onze club heeft een **register** (verplicht) waarin alle verwerkingsactiviteiten (ledenregistratie, registratie activiteiten…) worden behandeld.
4) Onze club heeft geschreven **overeenkomsten** met verwerkers.
5) Onze club **beveiligt** (de verwerking van) **persoonsgegevens**.
6) Onze club werkt **enkel** met de **noodzakelijke gegevens** voor de uitvoering van haar doeleinden.
7) Onze club **vraagt actief toestemming** voor het gebruik van gegevens als dit nodig blijkt (wetsgronden).
8) Onze club houdt de persoonsgegevens maar bij **tot zolang** dit **nodig blijkt**.
9) Onze club **informeert** duidelijk over het gebruik van gegevens, o.a. via een duidelijke **privacyverklaring**.
10) Onze club kan **snel reageren** bij vragen van leden/deelnemers rond het gebruik van hun gegevens.
11) Onze club kan **direct reageren bij verlies** van persoonsgegevens (een datalek).

2 Hoe implementeren we de Verordening in onze club?

Voor het implementeren van de Verordening wordt ons aanbevolen een STAPPENPLAN te volgen.



2.1 stap 1 BEWUSTMAKING

1) We bespreken met het bestuur en **Informeren** de medewerkers in onze club die met gegevens werken over:
   a) Het belang van privacy van onze leden, vrijwilligers, deelnemers,…
   b) De stappen om onze club in regel te brengen.
   c) De beveiliging van persoonsgegevens.

2.2 stap 2 INVENTARIS

1) We maken een lijst met welke gegevens wij waarom gebruiken. De inventaris is geen verplicht document maar helpt wel om een goed zicht te krijgen over de gegevensverwerking in onze club. Het is ook een goede basis voor de opmaak van ons register.

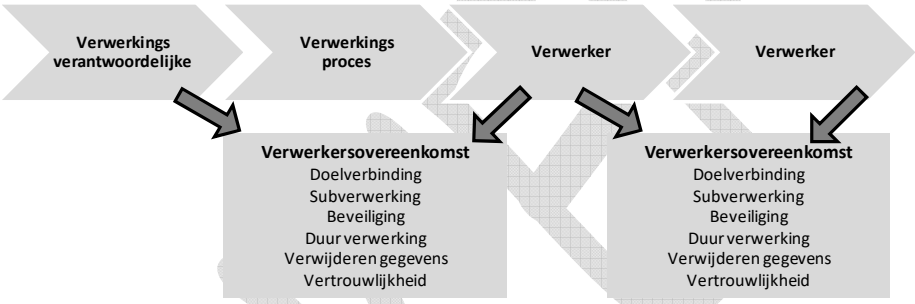
2.3 stap 3 ANALYSE EN MAATREGELEN

1) We gaan na hoe ver we staan en welke stappen we best nemen om de privacy van de gegevens van onze leden, vrijwilligers en deelnemers te beschermen.
2) We kijken na of:
   a) We de leden, deelnemers, vrijwilligers, partners duidelijk **informeren** (privacyverklaring).
   b) We een wettelijke **grond** hebben om gegevens te verwerken.
   c) We **niet te veel gegevens** opvragen en deze niet te lang bewaren.
   d) De gegevens voldoende worden **beveiligd**.
   e) De leden, vrijwilligers, partners, deelnemers, … de mogelijkheid hebben om hun gegevens in te zien, te corrigeren, te laten verwijderen, …

2.4 stap 4 REGISTER (verplicht document)

1) We maken een register op over onze gegevensverwerking.
2) Voorbeelden van verwerkingen:
   a) Opnemen van de persoonsgegevens van een nieuw lid in het ledenbestand.
      i) Doorsturen van bepaalde gegevens naar de federatie (VAL).
   b) Jaarlijks boeken van het lidmaatschapsgeld van het lid jaarlijks voor.
   c) Versturen van nieuwsbrieven aan de (jeugd)leden.
   d) Publiceren van foto's en video's van wedstrijden op onze verenigingswebsite en Facebook.
   e) Verwijderd van de gegevens uit het ledenbestand, nadat het lid is uitgetreden.

3) Voor de gegevensverwerking onderscheiden we meerdere rollen:
   a) **De verwerkingsverantwoordelijke**:
      i) Bepaalt welke gegevens worden verzameld en verwerkt.
      ii) Bepaalt doel en middelen gegevensverwerking.
      iii) Is verantwoordelijk.
      iv) Vraagt overeenkomsten aan verwerker.
      v) Houdt een register (verplicht) bij.
   b) **De verwerker(s)**:
      i) Handelt in opdracht van de verwerkingsverantwoordelijke en moet zich aan de afspraken houden (bv VAL, Alabus, cloud).
      ii) Houdt een register (verplicht) bij.
   c) **De derde(n)**:
      i) Ontvangt gegevens maar verwerkt ze niet in jouw opdracht.
   d) **De betrokkene**:
      i) De persoon wiens gegevens je verwerkt.



2.5 stap 5 PRIVACYVERKLARING (verplicht document)

1) We maken een privacyverklaring op.
2) We nemen hier volgende zaken zeker in op:
   a) WELKE gegevens worden verwerkt?
   b) WAAR krijgt of verzamelt onze club de gegevens?
   c) WAAROM worden de gegevens bewaard?
   d) WIE verwerkt in onze club gegevens?
   e) WIE krijgt de gegevens?
   f) WAT wordt precies HOE, WAAR en HOELANG bewaard?
   g) HOE worden gegevens beveiligd?
   h) HOE zorgt onze club voor de uitoefening van de rechten van betrokkenen?

2.6 stap 6 VRAGEN VAN LEDEN of DEELNEMERS

1) Onze leden, vrijwilligers en deelnemers hebben rechten. We zorgen als club dat we kunnen reageren bij vragen van leden.
2) De belangrijkste rechten van leden, vrijwilligers of deelnemers voor onze werking zijn:
   a) recht op inzage en kopie.
   b) recht op aanpassing van de gegevens.
   c) recht op vergetelheid (verwijderen van gegevens), behalve wanneer deze nog nodig zijn voor bijvoorbeeld uitvoering contract,...
   d) recht op intrekken toestemming (bij toestemming als rechtsgrond).

2.7 stap 7 AANPAK DATALEK

1) Verlies van persoonsgegevens moeten we aangeven bij de privacycommissie.
2) We zorgen dat we klaar zijn bij een mogelijk datalek (verlies van persoonsgegevens).
3) We duiden een persoon aan die deze taak op zich neemt.
4) We zorgen dat iedereen in onze club weet tot wie hij zich moet richten.

3 Overzicht krijgen met een VERWERKINSREGISTER

1) We zijn verplicht zorgvuldig om te gaan met persoonsgegevens. De wet stelt daarvoor een aantal concrete eisen.
2) Om te achterhalen welke gevolgen dit heeft voor onze club, moeten we eerst grondig vaststellen hoe onze club persoonsgegevens zoal gebruikt.
3) Deze informatie leggen we vast in een verwerkingsregister (hierna: 'register'). Het bijhouden van een register is vanaf 25 mei 2018 wettelijk verplicht.

3.1 Wat is het nut van een register?

Een register komt van pas bij het stapsgewijs controleren van het privacybeleid binnen onze club. Zo kunnen we met het register bijvoorbeeld per verwerking nagaan of een gebruik van persoonsgegevens wel of niet is toegestaan en of de gebruikte gegevens niet te lang worden bewaard.

3.2 Welke informatie nemen we op in het register?

1) Het register is een schematisch overzicht met essentiële informatie over de verwerkingen van persoonsgegevens binnen onze club.
2) Het register geeft minimaal antwoord op de volgende vragen:
   a) Wat zijn de verschillende doeleinden waarvoor onze club persoonsgegevens verwerkt?
   b) Om welke persoonsgegevens gaat het?
   c) Op welke categorie personen hebben de gegevens betrekking (wie zijn de betrokkenen)?
   d) Hoe lang worden de betreffende persoonsgegevens bewaard?
   e) Verstrekt onze club persoonsgegevens aan derden, wie zijn dit en wat is het doel daarvan?
   f) Wat zijn in algemene bewoordingen de getroffen beveiligingsmaatregelen ter bescherming van de betrokken persoonsgegevens?
   g) Worden er persoonsgegevens doorgegeven aan of opgeslagen in landen buiten de Europese Economische Ruimte en/of internationale organisaties en, zo ja, welke landen en/of organisaties zijn dit?
3) Het is aanbevolen per verwerkingsdoel ook de volgende informatie op te nemen:
   a) Wie zijn binnen onze club belast met deze verwerking?
   b) Welke IT-systemen worden gebruikt bij deze verwerking?
   c) Hoe zijn betrokkenen geïnformeerd over deze verwerking?

3.3 Toepassing van het register

Hierna twee voorbeelden hoe het register kan ondersteunen bij het controleren of onze club voldoet aan de privacyregels.

3.3.1 Toepassing van het register (1): is het doel van de verwerking rechtmatig?

1) Persoonsgegevens mogen enkel worden verwerkt indien daarvoor een geldige 'grondslag' bestaat.
2) Onze club moet een verwerking in de praktijk meestal kunnen baseren op minimaal één van onderstaande gronden:
   a) De verwerking is noodzakelijk voor de uitvoering of de totstandkoming van een overeenkomst met de betrokkene (voorbeeld: het opnemen van een nieuw lid in de ledenadministratie);
   b) De verwerking is noodzakelijk voor de naleving van een wettelijke plicht (voorbeeld: de algemene fiscale bewaarplicht van zeven jaren);
   c) De betrokkene geeft toestemming voor de verwerking (voorbeeld: het plaatsen van foto's van (jeugd)spelers op sociale media); of
   d) De verwerking is noodzakelijk vanwege een gerechtvaardigd belang van onze club of van een derde partij (voorbeeld: het versturen van nieuwsbrieven aan leden door onze club).
3) Zijn alle toepasselijke grondslagen eenmaal opgenomen in het register, dan kan per verwerking worden vastgesteld of deze grondslag toereikend is of niet. Ontbreekt een geldige grondslag, dan weten we dat de verwerking moet worden gestaakt.

3.3.2 Toepassing van het register (2): wordt een juiste bewaartermijn toegepast?

1) Persoonsgegevens mogen in principe niet langer worden bewaard dan noodzakelijk is voor het beoogde doel, tenzij de wet bepaalt dat zij voor langere tijd moeten worden opgeslagen.
2) Hoe lang we persoonsgegevens bewaren, varieert in de praktijk nogal. Een structureel overzicht is daarom noodzakelijk. Een register helpt bij het aanbrengen van die structuur.
3) Voorbeelden van bewaartermijnen:
   a) Persoonsgegevens van een uitgetreden lid bewaren we in principe niet langer dan twee jaren na het einde van het lidmaatschap.
   b) Voor informatie die valt onder de fiscale bewaarplicht geldt een langere bewaartermijn, namelijk zeven jaren. Onze penningmeester bepaalt welke gegevens daaronder vallen.
   c) Sommige informatie zullen we voor statistische doeleinden langer bewaren. Dat mag, maar we zorgen wel dat deze langer bewaarde gegevens niet alsnog voor andere doeleinden worden gebruikt, en we onderzoeken in hoeverre we de gegevens kunnen 'anonimiseren'.

4 Maatregelen ter BEVEILIGING van persoonsgegevens

1) Indien je als clubmedewerker in aanraking komt (raadplegen – bewerken – verspreiden – opslaan – kwijtraken …) met persoonsgegevens van onze leden, vrijwilligers, sponsors, …, gelieve dan in de mate van het mogelijke de hierna vermelde maatregelen na te leven.
2) Tal van nuttige tips zijn terug te vinden op de website https://www.safeonweb.be/nl.

4.1 Organisatorische maatregelen

1) Invoeren/naleven van een geheimhoudingsplicht aan vrijwilligers/bestuurders.
2) Het veiligheidsbewustzijn van de vrijwilligers/bestuurders creëren/onderhouden door periodieke opfrissessies.
3) Adreslijsten/deelnemerslijsten en/of gegevensdragers met persoonsgegevens niet laten rondslingeren.
4) Beperken van de info op deelnemerslijsten/formulieren.
5) Verwijzen naar de privacy verklaring op de aansluit- en inschrijvingsformulieren.
   "AS Rieme vzw verwerkt uw gegevens conform onze privacyverklaring".
   a) Op de website kan dit met een hyperlink, onderaan iedere pagina, naar de privacyverklaring.
   b) Bij ter plaatse aansluiten/inschrijven verwijzen we op het formulier naar de (beknopte) privacyverklaring, die we ter plaatse beschikbaar houden.
6) Geen gevoelige bestanden (met o.a. persoonsgegevens) per email versturen.
7) Surf niet naar websites met persoonlijke of belangrijke informatie via openbare computers of een openbaar wifi-netwerk. Hackers zullen er maar wat graag misbruik van proberen maken, aangezien ze dan ineens massaal veel gegevens in de wacht kunnen slepen. Vermijd bijvoorbeeld bankverrichtingen.

4.2 Technische maatregelen

4.2.1 Doe regelmatig (automatisch) updates

1) Om mogelijke lekken in de veiligheid van je computer, smartphone of tablet te vermijden (zowel bij Windows en Mac), installeer je altijd het best de laatste update van je besturingssysteem.
   a) Besturingssysteem (Windows, Apple, Android, iOS-toestel, ...).
2) Internet browser (Chrome, Firefox, Internet Explorer, Safari, Opera ...).
3) Virusscanner (MS Security Essentials, Bullguard, Norton, AVG, McAfee, ...).
4) Adobe PDF Reader.
5) Adobe Flash Player.
6) Java.
7) Microsoft Office.
8) Apps op je mobiele Android-toestel.
9) Apps op je mobiele iOS-toestel.

4.2.2 Gebruik wachtwoorden op bestanden met persoonsgegevens

1) Lange tijd werd gedacht dat het ideale wachtwoord bestond uit een willekeurige combinatie van cijfers en (hoofd)letters. Blijkt nu dat de huidige systemen van hackers en fraudeurs dergelijke logins gemakkelijk kunnen kraken.
2) **Wat dan wél veilig is?**
   Experts beweren dat lange wachtwoorden bestaande uit zo'n vier woorden veel moeilijker zijn om te kraken. Het zou zo'n 550 jaar duren om het wachtwoord 'correcthorsebatterystaple" te kraken, terwijl een wachtwoord met cijfers en letters, en dat als veilig werd beschouwd, al in drie dagen gehackt kan worden.
3) Gebruik niet hetzelfde wachtwoord voor àl je applicaties. Of het nu om je e-mailaccount, online winkelpasje of Netflix-account gaat, de regel geldt altijd: hoe meer variatie, hoe beter.
4) Wijzig de wachtwoorden na bepaalde periode (bvb jaarlijks).

4.2.3 Gebruik een wachtwoordkluis

1) Een mens heeft zoveel wachtwoorden en log-ins te onthouden dat hij geneigd is zich dan maar overal van dezelfde aanmeldgegevens te bedienen. Geen goed idee uiteraard, ingeval dat – ene – wachtwoord in verkeerde handen terecht komt! Een wachtwoordkluis biedt een uitweg uit deze impasse.
   "De enige wijze om veilig met wachtwoorden om te gaan is om voor elke site een ander wachtwoord te hebben en deze door een extern systeem willekeurig te laten samenstellen, op te slaan en veilig terug te geven."
2) **Hoe werkt een wachtwoordkluis?**
   Je creëert eerst een digitale kluis – het kunnen er overigens ook meerdere zijn – die je uiteraard met een stevig en complexe wachtwoord afschermt, waarna je binnen die kluis alle login's, wachtwoorden, id's en aanverwante informatie stockeert. De tool bewaart al die informatie dan in de kluis en versleutelt die met een stevige encryptie.
3) Een **Wachtwoordenkluis** (KeePass) werd geïnstalleerd/is toegankelijk **in DropBox**.
   a) Alle (Office) bestanden met persoonsgegevens werden voorzien van een wachtwoord.
   b) Het **gebruik van een kluis** zou nuttig zijn voor de medewerkers die in aanraking komen met persoonsgegevens.
      Dit zijn: secretaris, ledenbeheerder, penningmeester, kledijbeheerder, materiaalbeheerder, wedstrijdinschrijver.

4.2.4 Leer valse mails herkennen

1) Phishing is online oplichting door valse mails, websites of berichten.
2) **Hoe herken je valse mails?**
   a) **Afzender**
      Controleer het adres van de afzender. De naam van de afzender mag dan precies hetzelfde zijn als die van je bank of webwinkel, maar vaak is het gebruikte e-mailadres vaag of een afgeleide versie van een echte bedrijfsnaam of de naam van een instantie. Is het adres vaag of onduidelijk? Dan heb je waarschijnlijk met phishing te maken.
   b) **Aanhef**
      Word je met hele algemene termen, zoals 'Geachte heer/mevrouw' of 'Beste klant', aangesproken, let dan op. Bedrijven en instanties waar je klant bent, gebruiken meestal in ieder geval je achternaam in een e-mail of weten of je een man of een vrouw bent.
   c) **Vragen naar persoonsgegevens**
      In veel nepmails staat het verzoek om je persoonsgegevens 'te controleren', 'bij te werken' of 'aan te vullen'. Je moet dan op een link klikken om dit te doen. Doe dit nooit zomaar. Je bank, verzekeringsmaatschappij en overheidsinstanties vragen nooit op deze manier naar persoonsgegevens. Bel het bedrijf of de instantie liever eerst op om te controleren of ze de e-mail wel zelf hebben verstuurd. Gebruik hiervoor nooit de contactgegevens in de e-mail, maar zoek deze zelf op.
   d) **Taalgebruik en vormgeving**
      De huidige generatie nepmails staan allang niet meer bol van de taal- en spelfouten. Ook de gebruikte logo's en foto's worden steeds professioneler. Lees en bekijk de e-mail goed om te zien of je toch geen onregelmatigheden tegenkomt. Je kunt ook een eerdere mail van een bedrijf of instantie ernaast leggen ter vergelijking.

e) **Links**
Links in nepmails kunnen ervoor zorgen dat er schadelijke software op je computer wordt geïnstalleerd of dat je naar een valse website wordt geleid. Klik dus nooit zomaar op de links in een e-mail die je niet vertrouwt. Controleer het adres van de link door, zonder erop te klikken, de cursor van je muis op de link te zetten en te kijken welk adres er verschijnt.

f) **Bijlage**
Een bijlage in een nepmail kan ervoor zorgen dat er schadelijke software op je computer wordt geïnstalleerd. Open dus nooit zomaar een bijlage van een e-mail die je niet vertrouwt. Een zip-bestand is altijd verdacht aangezien bijvoorbeeld facturen en aanmaningen nooit op deze manier worden verstuurd. Verwacht je toch een bestand? Neem dan contact op met de afzender om te vragen wat en hoe ze iets precies verstuurd hebben. Gebruik ook hiervoor nooit de contactgegevens in de e-mail, maar zoek deze zelf op.

4.2.5 Maak regelmatig back-ups

1) Op een computer staan vaak **bestanden die je niet wilt verliezen**. Maar er kan altijd iets met je computer mislopen. Een technisch defect of een virus kunnen jouw bestanden beschadigen of zelfs verwijderen. Daarom is het belangrijk om er een reservekopie van te maken. En dat doe je als je een back-up maakt!
2) **Wat is een back-up precies?**
Een back-up is een reservekopie van jouw belangrijke bestanden.
3) **Waarvan moet je een back-up maken?**
Je maakt best een kopie van jouw belangrijke bestanden, o.a. deze met persoonsgegevens, en ook van jouw mails.
4) **Hoe doe je dat?**
Jouw back-up drager kan een CD, een DVD, een USB stick, een externe harde schijf … zijn. Je kopieert uw belangrijke bestanden naar uw back-up gegevensdrager.
5) **Neem regelmatig een back-up.**
   a) Neem **dagelijks** een back-up van uw belangrijke documenten waar je dagelijks aan werkt.
   b) Neem wekelijks of maandelijks een back-up van uw documenten waar je slechts af en toe (bvb wekelijks) aan werkt.
   c) Neem steeds een back-up voor je een nieuw programma of een belangrijke update installeert of wanneer je jouw computer in herstelling geeft.

4.3 Mogen persoonsgegevens op privéapparatuur worden geplaatst?

1) Het is niet ongebruikelijk onze bestuurders/vrijwilligers bij de vervulling van verenigingstaken gebruik maken van privéapparatuur. Dat is in principe mogelijk, maar onze club blijft verantwoordelijk voor het veilige verloop van dit gebruik.
2) Overweeg in ieder geval het invoeren van de volgende regels:
   a) De gebruiker moet antivirussoftware installeren en deze regelmatig updaten;
   b) De gebruiker moet deugdelijke toegangscodes instellen;
   c) Vermijd opslag op lokale harde schijven indien gebruik kan worden gemaakt van webomgevingen (bijv. Google Apps, Office 365, online verenigingsadministratie etc.);
   d) Zorg dat te allen tijde een deugdelijke back-up beschikbaar blijft van de gegevens die op de privéapparatuur worden verwerkt; en
   e) Beëindigt iemand zijn of haar verenigingstaken, zorg er dan voor dat deze persoon niet langer toegang heeft tot de gegevens.

5 De PRIVACYVERKLARING van AS Rieme

1) Een privacyverklaring moet niet goedgekeurd worden. Het gaat om een eenzijdige verklaring van onze club waarin we bepalen hoe er met de persoonsgegevens zal worden omgegaan.
2) Onze club bezorgt/verwijst naar de privacyverklaring vooraleer de persoonsgegevens verwerkt worden.

5.1 De beknopte privacyverklaring

1) De beknopte privacyverklaring is opgemaakt in de richtlijn **RL 70 'De beknopte privacyverklaring van AS Rieme'**.

'Uw persoonsgegevens worden verwerkt door AS Rieme vzw, Jacob van Arteveldelaan, 3 te 9940 Ertvelde, riem@val.be, voor het ledenbeheer, de aanschaf van clubkledij en de organisatie van activiteiten op basis van de contractuele relatie als gevolg van uw inschrijving en voor direct marketing (om u op de hoogte te houden van onze activiteiten) op basis van ons gerechtvaardigd belang om sport aan te bieden.
Indien u niet wil dat wij uw gegevens verwerken met het oog op direct marketing, volstaat het ons dat mee te delen op (riem@val.be). Via dat adres kan u ook altijd vragen welke gegevens wij over u verwerken en ze verbeteren of laten wissen, of ze vragen over te dragen. Een meer uitgebreid overzicht van ons beleid op het vlak van verwerking van persoonsgegevens vindt u op (http://www.asrieme.be).'

5.2 De uitgebreide privacyverklaring

1) De privacyverklaring is opgemaakt in de richtlijn **RL 71 'De privacyverklaring van AS Rieme'**.

6 Wat moet onze club doen in geval van een DATALEK?

1) Leidt een beveiligingsincident tot de vernietiging, verlies, wijziging of ongeoorloofde verstrekking/toegang, dan is er mogelijks sprake van een datalek.
2) Als het datalek (waarschijnlijk) geen nadelige gevolgen heeft voor de betrokken personen, moet het lek enkel tijdig worden gemeld bij de Autoriteit Persoonsgegevens.
3) Heeft het lek bovendien een hoog risico op nadelige gevolgen voor de personen wiens gegevens het betreft, dan moet het incident ook aan deze personen worden gemeld.
4) Blijkt een datalek achteraf ten onrechte niet tijdig te zijn gemeld, dan kan dit leiden tot oplegging van een fikse boete.

6.1 Aangifte van een datalek

1) Het formulier voor de aangifte van een datalek is opgemaakt in de richtlijn **RL 72 'Aangifteformulier datalek'**.
2) Als er zich binnen onze club een verlies van persoonsgegevens voordoet, spreekt men van een datalek. Dit kan onder meer gebeuren wanneer er een laptop wordt gestolen, wanneer je computer wordt gehackt, wanneer je een usb-stick met alle adressen van de leden verliest, enz.
3) Onze club houdt een intern bestand bij met alle incidenten van mogelijke lekken van gegevens.
4) Bij een datalek moet de verwerkingsverantwoordelijke van onze club de Gegevensbeschermingsautoriteit (GBA) inlichten binnen de 72 uur na vaststellen van het datalek, tenzij het niet waarschijnlijk is dat de inbreuk in verband met persoonsgegevens een risico inhoudt voor de rechten en vrijheden van natuurlijke personen. Niet naleven van de meldplicht bij een datalek, kan stevige boetes met zich meebrengen.