Voorstel van nota voor de clubs i.v.m. GPDR

1. Doelstelling van deze nota

Deze nota heeft als bedoeling een leidraad te geven bij de toepassing van GDPR binnen een Rotary club context. Uiteraard vervangt dit niet de bestaande wetteksten, noch is deze nota exhaustief. Daarenboven behandelt deze nota enkel de "normale" clubwerking; jeugduitwisselingsinitiatieven (e.g. YEP) vallen niet onder deze nota, aangezien hier specifieke persoonsgebonden gegevens zoals medische dossiers etc. Een andere aanpak vereisen. We verwijzen hieromtrent naar de nota's van RI die de GDPR context in deze gevallen duiden.

2. Wat is GDPR ?

GDPR is de afkorting van General Data Protection Regulation. Dit is een aangepaste Europese wetgeving die gaat over de bescherming van persoonlijke gegevens, en die van kracht werd op 25/5/2018 in alle landen van de Europese lidstaten. Ze vervangt aldus de Belgische wetgeving die sinds 1992 de privacy vereisten regelde. Ook niet Europese organisaties dienen zich hieraan te houden indien zij gegevens verwerken van Europese burgers.

In essentie geeft deze wet burgers het recht om te bepalen of, wanneer , hoe en aan wie zijn of haar gegevens en informatie worden verstrekt en waartoe die gegevens mogen gebruikt worden.

In deze wet wordt de definitie van "persoonlijke gegevens" sterk uitgebreid. Genetische, sociale, culturele, mentale en economische gegevens vallen voortaan onder dit begrip "persoonlijke gegevens".

Elk bedrijf of organisatie is voortaan verplicht de persoonlijke data te beveiligen. Je bent als bedrijf of organisatie hoofdelijk verantwoordelijk voor de data die je verwerkt en bewaart. De wet behandelt vier grote thema's :

a. **Transparantie** : wanneer gegevens van een persoon bewaard worden of gebruikt worden, dan moet men daar vooraf toestemming voor hebben van de persoon in kwestie.
b. **Data overdracht** : op eenvoudig verzoek van de betrokkene kunnen gegevens overgedragen worden naar een andere organisatie of gebruiker
c. **Recht om verwijderd te worden** : bedrijven en organisaties moeten persoonlijke gegevens wissen als de betrokkenen daarom vraagt en als er geen geldig tegenargument gegeven kan worden (om deze niet te wissen).
d. **Meldplicht bij datalekken** : verplichting datalek te melden binnen de 72 uur, tenzij wordt aangetoond dat het lek geen gevaar is voor de verzamelde persoonsgegevens

Men maakt een onderscheid tussen "gewone" persoonsgegevens en "bijzondere categorieën" van persoonsgegevens.

Onder "**gewone**" persoonsgegevens vallen bijv. :

+ naam
+ adres
+ telefoon
+ e-mail
+ foto
+ ip-adres
+ etc..

Onder "**bijzondere categorieën**" vallen bijv. :

+ ras of etnische afkomst

+ politieke of religieuze codering
+ biometrische of genetische gegevens
+ medische gegevens
+ seksuele geaardheid
+ rijksregisternummer
+ strafrechtelijke feiten
+ etc.

Voor deze laatste categorie worden extra voorwaarden opgelegd. We verwijzen naar de specifieke nota's van RI om na te gaan wat de GDPR vereisten zijn in deze gevallen.

3. Is dit relevant voor uw club ?

Uiteraard ! Hierbij is het irrelevant of uw club een feitelijke vereniging is of een VZW of een andere rechtsvorm heeft. Uw Rotary club valt integraal onder de GPDR regels, aangezien zij persoonsgegevens beheert en verwerkt.

Het belangrijkste administratief systeem dat door alle Rotary clubs gebruikt wordt binnen Belux, is HARMONY. Voor dit systeem is er – vanuit RBS – reeds bij de opstart van HARMONY en eveneens recent actie genomen om maximaal in orde te zijn met de GDPR regelgeving (zie volgend punt).

Bij de opstart van HARMONY in uw club is er een document ondertekend door de toenmalige Voorzitter (of Secretaris) die specifieerde hoe de persoons-gegevens gebruikt worden binnen HARMONY. Dit document specifieerde o.a. :

+ de doelstellingen van HARMONY gebruik
+ toegangsrecht en gebruikersrecht
+ het gebruikersprofiel
+ de aansprakelijkheid van de verschillende actoren
+ het intellectuele eigendom

In feite is er op dat moment geanticipeerd op de huidige wetgeving, en volstaat dit document ook vandaag om "compliant" te zijn.

4. De belangrijkste administratieve tool : HARMONY

RBS heeft bij opstart van HARMONY reeds heel wat administratieve stappen doorlopen, resulterend in verschillende contracten met verschillende dataverwerkers (binnen- en buiten Europa).

Anticiperend op de invoering van GDPR heeft RBS een "privacy compliance" scan laten uitvoeren door een gespecialiseerd bureau. Hieruit zijn een aantal werkpunten naar voor gekomen, waar RBS nu en in de komende maanden de nodige acties zal ondernemen om hieraan te remediëren. De uitslag van deze privacy compliance scan was trouwens zeer positief, en situeert Rotary Belux bovenaan de organisaties die deze scan reeds lieten doorvoeren.

Conclusie: voor wat betreft de verwerking van de gegevens in HARMONY , en de transfert naar Rotary International, hoeft U zich geen zorgen te maken. RBS volgt dit verder op.

5. Welke maatregelen kan U zelf nemen ?

Wat volgt zijn enkele aanbevelingen om de risico's op een "non-compliance" zo klein mogelijk te maken :

+ U hebt er belang bij dat de gegevens van uw leden niet te pas en te onpas door de Rotariërs van uw club gebruikt of misbruikt worden.

Een duidelijk communicatie-plan, al dan niet onderdeel van het Huishoudelijk Reglement van uw club kan hierbij helpen.
Zo is het sterk aan te bevelen dat leden zich eerst wenden tot de bevoegde commissievoorzitter en/of het bestuur van de club met vragen en/of opmerkingen.
Ook het correct gebruik van communicatiemiddelen kan onderdeel uitmaken van dergelijk communicatie-plan. Zo is bv. af te raden om groepsdiscussies via e-mail te voeren, of club-interne aangelegenheden publiek te maken op social media. Zo kan bv. ook expliciet afgesproken worden dat alle formele communicatie binnen de club alleen van de clubsecretaris kan komen, of dat de maandafrekening alleen van de penningmeester kan komen. Goede afspraken maken immers goede vrienden.

+ Als U vanuit uw club mails verstuurt naar alle clubleden, dan is het aangewezen de adressen in bcc: te plaatsen

+ Mails met familiale doeleinden (aankondiging geboorte, sterfgeval, ziekte , etc.) vallen niet onder GDPR

+ Zoals in het verleden is het gebruik van adressen (al dan niet elektronisch) uit het (gedrukt of online) jaarboek, zonder toestemming van RBS , niet toegelaten. Indien één van uw leden dit toch doet, dan vormt dit een inbreuk op GDPR die U best bij RBS meld.

+ Ook voor het versturen van mailings naar (alle) leden van een andere club, vraagt U best aan de Secretaris of de Voorzitter van de desbetreffende club dat zij uw bericht in hun club verder verspreiden.

+ Wanneer U uitnodigingen van activiteiten naar derden verstuurt , dan hebt U in principe hun toestemming vooraf nodig dat U dergelijke mails mag/kan versturen. Het is dus belangrijk van U daarop te organiseren. Bij opvragen van persoonsgegevens in een website, vermeldt U best dat de verstrekker van de gegevens

akkoord gaat met het gebruik van zijn/haar gegevens in het kader van Rotary activiteiten.

6. En wat zegt Rotary Internationaal ?

Rotary International stelt expliciet dat zij haar privacy bepalingen aangepast heeft aan de vereisten van GDPR. De privacy policy van RI is te vinden op de website www.rotary.org .

Rotary International stelt geen templates ter beschikking, omdat de verschillen tussen districten en clubs zo groot zijn , dat een template niet meer relevant zou zijn voor de specifieke situaties.

7. Wat indien U (persoonsgebonden) gegevens gebruikt in andere toepassingen ?

In principe moet U dan zelf instaan om compliant te zijn met GDPR. Dit houdt o.a. in dat U :

+ een data register aanlegt. Dit register beschrijft in detail welke gegevens er door de toepassing(en) gebruikt worden

+ aangeeft hoe je deze gegevens verzamelt, hoe je deze gebruikt en hoe je deze gegevens beveiligd

+ een rechtvaardigheidsgrond opstelt. Deze geeft aan waarom U bepaalde gegevens opvraagt (en dit per "veld")

+ aangeeft welke derden deze gegevens ter beschikking krijgen en/of verder verwerken

+ ervoor zorgt dat diegene die de gegevens verstrekt, ondubbelzinnig akkoord gaat met het gebruik ervan

+ ervoor zorgt dat elke betrokkene inzicht kan krijgen in wat voor hem/haar opgeslagen is , en de mogelijkheid krijgt te vragen naar een aanpassing of schrapping ervan

+ ervoor zorgt dat de gegevens technisch voldoende beveiligd zijn. Naargelang de gevoeligheid van de opgeslagen data kan dit gaan van een wachtwoord beleid, over een firewall , encryptie en/of multifactor-authentificatie.

+ bij inbreuken, dat U deze meldt aan de bevoegde toezichthoudende authoriteit.

8. Hebt U nog vragen ?

Dan kan U deze steeds stellen aan RBS (Rotary Belux Services) via e-mail : gdpr@rotarybeluxservices.org