GDPR-tillämpning i D2405

Personuppgiftsansvar

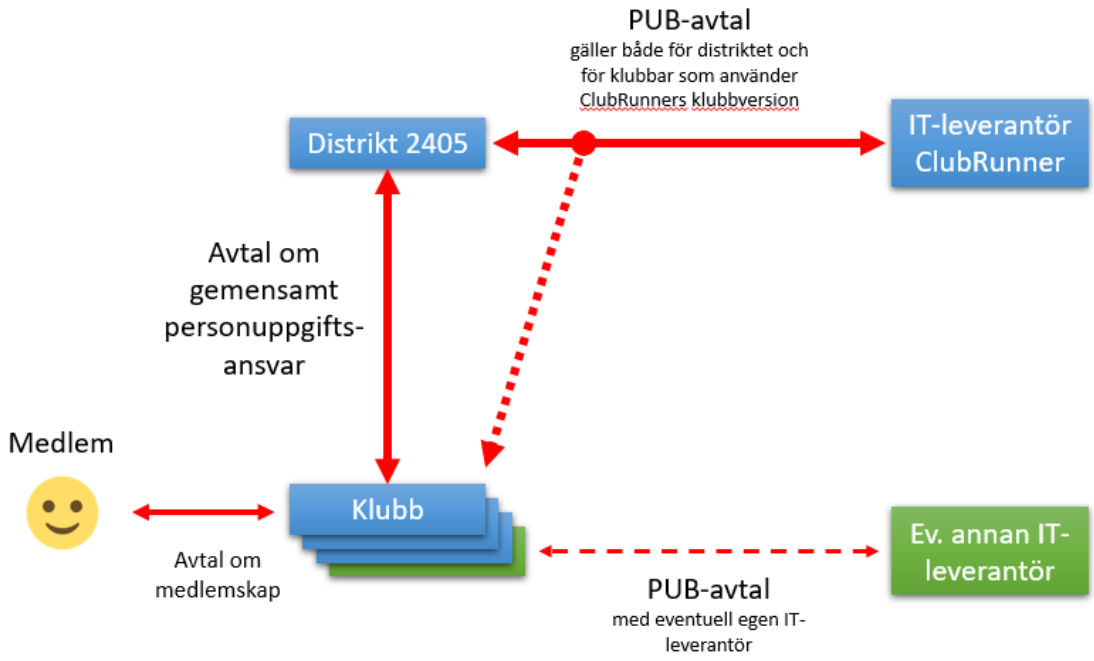
Varje klubb är personuppgiftsansvarig, men eftersom distriktet också behandlar medlemmarnas personuppgifter för vissa ändamål finns avtal mellan D2405 och klubb om gemensamt personuppgiftsansvar, se bilaga 1.

Avtalsstruktur

Behandling av personuppgifter för Rotarymedlemmar i distrikt 2405 är GDPR-säkrad genom:

- Avtal om gemensamt personuppgiftsansvar mellan distrikt och klubb.
  Avtalet tydliggör respektive parts ansvar för GDPR-relaterade skyldigheter, bl a att ClubRunner-klubb uppdrar åt distriktet att teckna PUB-avtal med ClubRunner.
- Personuppgiftsbiträdesavtal (PUB-avtal) med IT-leverantören ClubRunner, gäller för distriktets hantering av personuppgifter för medlemmar i alla distriktets klubbar, samt för klubbar som använder ClubRunners klubbversion.

Klubb som anlitar annan IT-leverantör än ClubRunner ansvarar själv för att teckna PUB-avtal med leverantören.



Rättslig grund

Den rättsliga grunden för behandling av medlemmars personuppgifter är för de flesta ändamål avtalet om medlemskap: för att fullgöra avtalet måste klubben behandla personuppgifter för att föra medlemsregister, administrera medlemsavgift, informera via utskick, m m, - distriktet måste behandla personuppgifter för att göra utskick, ge stöd till klubbar m m. Samtycke behövs inte, annat än för specifika ändamål som går utöver det grundläggande avtalet om medlemskap.

För överföring av personuppgifter till RI/MyRotary är den rättsliga grunden att klubben har ett berättigat intresse (s k intresseavvägning) till följd av sina förpliktelser till RI att hålla medlemsregistret i MyRotary uppdaterat.

För icke-medlemmar är samtycke den rättsliga grunden för att behandla personuppgifter vid bl a prenumeration på nyhetsbrev.

Personuppgiftsbiträden

ClubRunner som IT-leverantör
D2405 som använder ClubRunners distriktsversion och distriktets klubbar som använder ClubRunners klubbversion har personuppgiftsbiträdesavtal med ClubRunner i Kanada gällande ClubRunner och deras underbiträden, se bilaga 2.

Avtalet är togs fram 2022 av ClubRunner med stöd av svensk GDPR-expertis och innehåller bl a EU:s uppdaterade standardavtalsklausuler (2021) för så kallade dataimportörer, dvs tjänsteleverantörer med huvudsäte utanför EU.

ClubRunner använder f f a USA-baserade Microsofts molntjänst Azure. Microsoft är certifierat enligt EU-U.S. Data Privacy Framework Program och uppfyller därmed EU-kommissionens krav på ”adekvat skyddsnivå”. Samma gäller e-postleverantörerna GoDaddy och Sendgrid i USA. En ytterligare underleverantör för e-post är MailJet som är Frankrikebaserat och har sina servrar i EU-länder.

Annan IT-leverantör till klubb
Om en klubb använder annan IT-leverantör, t ex Polaris (tre klubbar i D2405), är det klubbens ansvar att teckna personuppgiftsbiträdesavtal med leverantören. Läs mer på D2405-supportsidan GDPR.

Integritetspolicy

Integritetspolicy publiceras på distriktets respektive klubbs webbplats:

- Integritetspolicy D2405 resp Cookie policy
- Integritetspolicy Värmdö Skärgård RK (som exempel på klubb).

Bilagor

1. Avtal om gemensamt personuppgiftsansvar
2. PUB-avtal: Data Processing Agreement

Fördjupning

- Överföring till USA.
  Integritetsmyndighetens (IMY) information.
- EU-U.S. Data Privacy Framework
  Microsofts information om implementering av EU-U.S. DPF.
- The General Data Protection Regulation (GDPR) and ClubRunner.
  ClubRunners information om GDPR m m.
- Standard contractual clauses for data transfers between EU and non-EU countries.
  EU-kommissionen beskriver de uppdaterade standardavtalsklausulerna från 2021.

Värmdö som ovan
Anders Tihkan (Värmdö Skärgård RK)
LinkedIn

Överenskommelse om gemensamt personuppgiftsansvar

enligt artikel 26 dataskyddsförordningen (GDPR) mellan
[*klubbnamn*] Rotaryklubb (”Klubben”) och Rotarydistrikt 2405 (”Distriktet”).

Bakgrund och ändamål

Då medlemmarnas personuppgifter hanteras av såväl Klubben som Distriktet är båda parterna gemensamt personuppgiftsansvariga enligt GDPR. I detta avtal fastställs därför respektive parts ansvar för att fullgöra skyldigheterna enligt GDPR.

Distriktet har av Infotech Business Center Inc. upphandlat applikationen ClubRunner som IT-stöd för Distriktet och dess Klubbar. I applikationen behandlas personuppgifter dels för medlemmar i Rotary, dels för andra personer med intresse för Klubbens och Distriktets verksamhet.

Distriktet använder personuppgifterna huvudsakligen för utskick av information rörande Rotarys verksamhet.

Klubben använder personuppgifterna huvudsakligen för att administrera klubben och medlemskapet samt för att skicka ut information om sin verksamhet och ta emot anmälningar till evenemang etc.

Fördelning av ansvar mellan Klubben och Distriktet

Distriktet tecknar personuppgiftsbiträdesavtal med Infotech Business Center Inc. enligt artikel 28 GDPR. Avtalet omfattar alla instanser i distriktet som använder ClubRunner.

Om klubben har annan leverantör än ClubRunner för att behandla personuppgifter ansvarar klubben för att teckna personuppgiftsbiträdesavtal med leverantören.

Klubben ansvarar för sitt personregister och är ansvarig för att hålla personuppgifterna uppdaterade och skyddade i enlighet med GDPR. Distriktet ska informera klubben om man får kännedom om felaktiga personuppgifter.

Klubben är medlemmens kontaktpunkt för dataskyddsfrågor.

Såväl Klubben som Distriktet ska iaktta tekniska och organisatoriska åtgärder för att skydda de registrerades personuppgifter.

Klubben aktiverar pseudonymisering eller motsvarande av f d medlemmar 3 – 4 månader efter utgången av det Rotaryår då medlemskapet upphörde, förutsatt att Klubben inte har ekonomiska eller andra krav på medlemmen som motiverar fortsatt registrering av personuppgifterna. Distriktet kan på klubbens begäran göra pseudonymiseringen för klubb som använder ClubRunner.

Klubben och Distriktet ska informera varandra vid personuppgiftsincident innan eller samtidigt som incidenten anmäls till IMY och berörda medlemmar.

Beslutsordning

Denna överenskommelse upprättas och blir gällande för båda parter genom att Klubbens president anger i Distriktets onlineformulär att Klubben accepterar överenskommelsen.

Bilaga 2

ClubRunner

Data Protection Agreement

Pursuant to article 28 GDPR, and including the EU commission Standard contractual clauses for the transfer of data to third country pursuant to Regulation (EU) 2016/679

Updated: 2022-04-28

THE PARTIES

The Customer, as stated in the Service agreement (the "Controller", the "data exporter"), established in the EU/EEA

ClubRunner, (the "Processor", the "data importer" when acting as processor and the "data exporter" when transferring data to a sub-processor)

PART ONE - GENERAL TERMS

1 INTRODUCTION

1.1 The parties agree that the ClubRunner Data Protection Agreement ("DPA" or "Agreement") sets forth their obligations with respect to the processing of Customer Personal Data in connection with the ClubRunner service (the "Service"). ClubRunner makes the commitments in this DPA to all non-enterprise customers using the Service. Separate terms, including different privacy terms, govern Customer's use of non-ClubRunner products.

1.2 This DPA governs only matters concerning the Processor's processing of personal data in conjunction with the Service. Annex I and II states the details of the processing of personal data by the Processor and constitutes a part of the Agreement. The Parties shall, at the latest at the signing of the Agreement ensure that Annex I and II are correctly filled in.

1.3 In the event of any conflict or discrepancy between the provisions of this Agreement and the Service Agreement, the provisions in this Agreement shall prevail. In the event of any conflict or discrepancy between the provisions of the Annex I and II and this Agreement, the Annex specification shall prevail. In the event of conflict between the Standard Contractual Clauses and any other provisions in the Service agreement or this DPA, the Standard Contractual Clauses shall prevail.

1.4 The DPA including the Standard Contractual Clauses and appendices are set up to fulfill the requirements of the General Data Protection Regulation 2016/679 (GDPR). The

Agreement enters into force at signing of the Service Agreement and replaces any previous agreements regarding processing of personal data between the Parties.

1.5 In addition to governing the Processor's processing of the personal data in the Service, the purpose of this Agreement is to assure that security and confidentiality is maintained in relation to the personal data when the Controller engages a Processor to process the personal data.

1.6 The Agreement means that the Processor, in accordance with the provisions of the GDPR, processes personal data for which the Controller is responsible. Article 28 GDPR requires that a written agreement is concluded between the controller and the processor.

2 DEFINITIONS

2.1 The "Applicable Data Protection Laws" means certain laws, regulations, regulatory frameworks, or other legislations relating to the processing and use of Customer Personal Data, as applicable to Customer's use of ClubRunner and the ClubRunner Service, including the EU General Data Protection Regulation 2016/679 ("GDPR"), along with any implementing or corresponding equivalent national laws or regulations, once in effect and applicable.

2.2 Unless otherwise specified in this section, the definitions in article 4 of the GDPR is applicable to this DPA.

2.3 "Customer Personal Data" means any Personal Data for which Customer is a Controller, whether supplied by Customer for processing by ClubRunner or generated by ClubRunner in the course of performing its obligations under the Service agreement. It includes data such as billing information, IP addresses, corporate email addresses, and any other Personal Data for which Customer is a Controller.

2.4 A "Data Breach" means a Personal Data Breach or any other confirmed or reasonably suspected breach of Customer's Protected Data.

2.5 "End User" means an individual Data Subject who controls a ClubRunner account and whose Personal Data is being transferred, stored, or processed by ClubRunner.

2.6 "Permitted Purposes" for data processing are those limited and specific purposes of providing the Service as set forth in the Annex I.B of this agreement.

2.7 "Protected Data" includes any Customer Personal Data processed by ClubRunner on behalf of Customer under the Agreement.

3 THE CONTROLLER

3.1 The Customer is, as Controller, responsible for ensuring and demonstrating that the processing of personal data is in accordance with the GDPR, the national data protection regulations and other binding regulations and decisions applicable to the processing of personal data within the Agreement ("Data Protection Legislation").

3.2 The Controller may provide further instructions that are legally required to comply with applicable Data Protection Legislation.

3.3 The Controller is responsible for giving the Processor instructions necessary for performing its responsibilities according to the Agreement and applicable Data Protection Legislation.

4 THE PROCESSOR

4.1 The Processor undertakes to comply with applicable Data Protection Legislation to the extent it is applicable to Processors and keep itself continuously updated in this respect.

4.2 The Processor undertakes to maintain complete, accurate, and up to date written record in accordance with article 30 GDPR, of all categories of processing activities carried out on behalf of Customer containing the information required under the Applicable Data Protection Laws. To the extent that assistance does not risk the security of ClubRunner or the privacy rights of individual Data Subjects, ClubRunner will make these records available to Customer on request as reasonably required, such as to help Customer demonstrate its compliance under the Applicable Data Protection Laws.

4.3 The Processor may not, without prior written consent from the Controller, process personal data for any other purpose than that set forth in the Agreement. The Processor undertakes to only process personal data, including transfers to a third country, in accordance with the Controller's written instructions in Annex I and II.

4.4 The Processor shall notify the Controller without undue delay if it believes an additional instruction violates applicable Data Protection Legislation. The Processor may suspend the performance of an instruction until the Controller has confirmed in writing that the additional instruction does not violate applicable Data Protection Legislation or the Controller has modified the instruction.

4.5 If the Processor lacks instructions it considers necessary to perform its duties, the Processor must inform the Controller without undue delay and await necessary instructions.

5 TRANSFERS OF PERSONAL DATA

5.1 The Controller ensure that there is a legal basis for transferring personal data to, or make available from, a location outside the EU or EEA by entering this DPA also entering into the EU Standard Contractual Clauses for the transfer of personal data to third countries.

5.2 The Processor shall be entitled to enter into such Standard Contractual Clauses with Sub-processors.

6 DATA PROTECTION

6.1 ClubRunner receives Customer Personal Data both from Customer and directly from Data Subjects who create End User accounts. If End-User accounts are registered as a consequence of the Customer agreement with ClubRunner the Customer is the Controller and the information registered is comprised by this DPA and the data is treated as Customer Personal Data.

6.3 ClubRunner will keep the Customer Personal Data accurate, or enable Customer to do so. ClubRunner will take commercially reasonable steps to ensure that any Protected Data it collects on Customer's behalf is adequate, relevant, and not excessive in relation to the purposes for which it is transferred and processed. In no event will ClubRunner intentionally collect Sensitive Data on Customer's behalf. Customer agrees that the ClubRunner Service is not intended for the storage of Sensitive Data; if Customer chooses to upload Sensitive Data to the Service, Customer must comply with Article 9 of the GDPR, or equivalent provisions in the Applicable Data Protection Laws.

6.4 Upon Customer's reasonable request, unless prohibited by law, ClubRunner will return, destroy, or deidentify all Customer Personal Data and related data at all locations where it is stored after it is no longer needed for the Permitted Purposes within thirty days of request. ClubRunner may retain Customer Personal Data and related data to the extent and for such period required by the Applicable Data Protection Laws, provided that ClubRunner will ensure that Customer Personal Data is processed only as necessary for the purpose specified in the Applicable Data Protection Laws and no other purpose, and Customer Personal Data remains protected by the Applicable Data Protection Laws.

6.5 The obligations and rights of Customer are set out in the Terms and Conditions, Privacy Policy and this Agreement. The ClubRunner Privacy Policy, publicly available at https://site.clubrunner.ca/page/privacy-policy-cr, provides detailed notice of ClubRunner's privacy and data use practices, including its use of cookies, its dispute resolution process, and further details about ClubRunner's GDPR compliance.

7 TECHNICAL AND ORGANIZATIONAL MEASURES

7.1 The Processor shall implement and maintain the technical and organizational measures specified in Annex II to ensure an appropriate level of security for the processing of personal data. The Controller guarantees that the technical and organizational measures are sufficient to fulfil the requirements stipulated by the applicable Data Protection Legislation.

7.2 The Processor shall ensure that persons authorized to process personal data have committed themselves to confidentiality or are covered by a legal confidentiality obligation.

7.3 The Processor shall not disclose the Controller's personal data to a third party unless authorized by the Controller or required by law, governmental- or supervisory authority decision. If the Processor is required by law, governmental- or supervisory authority decision to disclose the Controller's personal data to a third party, the Processor will notify the Controller prior to disclosure unless prohibited by law.

7.4 The Processor personnel have received adequate training on compliance with this Agreement and the Applicable Data Protection Laws.

8 THE PROCESSOR'S RESPONSIBILITY TO ASSIST THE CONTROLLER

8.1 The Controller is responsible for safeguarding the data subject's rights and responding to the data subject's requests for exercising its data subject's rights laid down in Chapter III GDPR, such as right to information, access to personal data, rectification, erasure and right to restrict the processing of personal data. If the data subject's request to exercise its data subject's rights is addressed directly to the Processor, the Processor shall inform the Controller without undue delay. The Processor furthermore undertakes to reasonably assist the Controller in fulfilling the data subject's rights.

8.2 The Processor furthermore undertakes, considering the type of processing and information available for the processor, to reasonably assist the Controller in ensuring compliance with the obligations relating to security of processing, notification of a personal data breach and the data protection impact assessment.

8.3 The Processor undertakes to, in accordance with the requirements stipulated in the Data Protection Legislation, cooperate with the Data Protection Authority in supervisory measures. If requests from the Data Protection Authority or other supervisory authorities regarding the Processors processing of personal data are aimed at the Processor, the Controller shall be notified without undue delay.

8.4 The Processor is entitled to a reasonable charge for assistance given to the Controller in accordance with the Agreement.

9 PERSONAL DATA BREACH

9.1 If the Processor becomes aware of a personal data breach the Processor shall, without undue delay notify the Controller. The notification shall at least contain the information needed for the Controller to fulfill its obligation to report the personal data breach to the Data Protection Agency. The Processor furthermore undertakes to assist the Controller in accordance with section 8.

10 REVIEWS AND AUDITS

10.1 The Processor will give the Controller access to all information required to demonstrate compliance with the requirements of the Data Protection Legislation and enable and contribute to audits, including inspections, conducted by the Controller or an auditor authorized by the Controller. Such authorized auditor may not be a competitor to the Processor.

10.2 Inspections may only be performed if the Controller informs the Processor in good time before the inspection and the Controller or auditor authorized by the Controller is bound by necessary confidentiality obligations. Inspections may furthermore only take place during the Processor's normal business hours, without disruption to the Processor's operational processes and provided that the Controller complies with the Processor's safety provisions at the place of inspection. The Controller shall document the result of the inspection and delete it when it is no longer necessary for the purpose of the inspection.

10.3 Each party bears its own costs for the Controller's audit of the processing of personal data performed by the Processor.

11 DAMAGES

11.1 A Data Subject or any other person who has suffered damage as a result of an infringement of the applicable Data Protection Legislation is entitled to compensation from the Controller or the Processor for the damage suffered. The Controller is liable for damage caused by processing that infringes the Data Protection Legislation. The Processor is liable for damage caused by processing where it has not complied with obligations specifically directed to processors, or where it has acted outside of or contrary to lawful instructions from the Controller.

11.2 The Controller or the Processor shall avoid liability for the damage suffered by the data subject if it shows that it is not in any way responsible for the event that caused the damage.

12 WHOLE AGREEMENT

12.1 This Agreement including the Standard Contractual Clauses and the Annex constitutes the whole Agreement between the Parties and supersedes and replaces earlier oral or written undertakings and covenants on the entire subject-matter of the Agreement.

No amendments or supplements to this Agreement will be valid unless made in writing and signed by duly authorized representatives of both Parties.

13 TERM OF AGREEMENT

13.1 This DPA applies between the Parties as long as the Processor processes personal data under the Service Agreement. If the Service Agreement is terminated and a new agreement of the same kind is concluded without a new DPA being concluded, this Agreement also applies to the new Service agreement. This Agreement can only be terminated on the conditions stipulated in the Service Agreement.

13.2 When the Processing has been terminated, or before that time upon request by the Controller, the Processor shall return or destroy all personal data it processes under the Service Agreement in accordance with Annex 1.B.

14 TERMINATION

14.1 In the event that the Processor is in breach of its obligations to maintain an adequate level of security or privacy protection, Customer may temporarily suspend the transfer of all Customer Personal Data or prohibit collection and processing of Customer Personal Data on Customer's behalf until the breach is repaired or the Agreement is terminated.

14.2 In addition to any termination rights Customer has under the Service agreement, Customer may terminate the Agreement in accordance with clause 16 of the Standard Contractual Clauses.

14.3 Failure to comply with the material provisions of this Agreement is considered a material breach under the Service Agreement.

14.4 In the event that changes in law or regulation render performance of this Agreement impossible or commercially unreasonable, the Parties may renegotiate the Agreement in good faith. If renegotiation would not cure the impossibility, or if the Parties cannot reach an agreement, the Parties may terminate the Agreement after thirty days.

15 EXECUTION

This Agreement has been executed as part of the Service Agreement between the Parties.

PART TWO - STANDARD CONTRACTUAL CLAUSES

TRANSFER OF PERSONAL DATA FROM THE CONTROLLER TO PROCESSOR

COMMISSION IMPLEMENTING DECISION (EU) of 4.6.2021on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) ([1]) for the transfer of data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9(a), (c), (d) and (e);

(iv) Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7

Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organizational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to

the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organizational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymization, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymization, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organizational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the

breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union ([2]) (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

a) The data importer has the data exporter's general authorization for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. ([3]) The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorized to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organizational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorized to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue

amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organization or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from

the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

(a) The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards ([4]);

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organizational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect

to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not

restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of Ireland.

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of the EU member state in which the data exporter is established.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

---

[1] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

[2] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

[3] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

[4] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

APPENDIX

ANNEX I

A. LIST OF PARTIES

Data exporter(s):

The Customer, as the Controller, is the signing party of the Service Agreement. Contact information is provided when signing the Service Agreement.

Activities relevant to the data transferred under these Clauses:

The Data Exporter uses the Service to administrate Club events, memberships, to contact members, to provide members, donors and benefactors with news and information about Club activities. The use implicates transferring personal data about members and administrators, donors and benefactors for administrative purposes.

Data importer(s): Name: Infotech Business Centre Inc. Operating as ClubRunner
Address: 2010 Winston Park Drive, Suite 200, Oakville, Ontario, Canada

Contact person's name, position and contact details: Halle Asterbadi, Chief Operating Officer (905) 829-5299

Activities relevant to the data transferred under these Clauses:

As a Processor to providing the Service as specified in the Service Agreement.

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

- Employees, volunteers and members of the controller
- Potential members
- Donors
- Other contacts and interested parties in contact with the Customer

Categories of personal data transferred

ClubRunner acknowledges that, depending on the controllers use of the Service, personal data from any of the following categories may be processed:

- Authentication data (for example, username, email, password);
- Contact information (for example, phone and email);

Unique identification numbers and signatures (IP addresses, unique identifier in tracking cookies or similar technology).

- Other unique identifying information. Data subjects may include more data such as real names and other personal information such as birth day.
- Log Information: about you're the use of the Services, including the type of browser used access times, pages viewed, IP address, general location, and the page you visited before navigating to our Services.
- Device Information: We collect information about the computer or mobile device you use to access our Services, including the hardware model, operating system and version.
- Cookies: We use cookies to store your login session and other information to make your navigation of our Services easier.

Sensitive data

The data importer does not intentionally collect or process any special categories of data in carrying out its services to the data exporter. The Controller is responsible for ensuring no sensitive data is uploaded in the service.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Personal Data is transferred at a frequency appropriate to the nature of the processing and can be one-off or continuous. Members have access to the information and the possibility to add, delete or alter the information registered about themselves. Other end users than members such as donors must contact the controller to alter or delete their information. For a complete deletion in the meaning of article 17 GDPR ClubRunner must be contacted.

Nature of the processing

ClubRunner provides a turn-key membership management and communications portal for club members to manage their data and activities. As part of initial setup, ClubRunner imports a club's membership details into the database, after which the administrator(s) may edit as needed, along with the member themselves. This core database is then used to enable other modules such as event registrations, volunteer signups, committee management, email newsletters, attendance tracking, and dues management to take place. Clubs add their data using the application for all modules, and to add new members. Removing data can be done either via the system or by contacting ClubRunner support with the request.

Purpose(s) of the data transfer and further processing
Purposes of the data transfer are to allow ClubRunner to provide the Services, which are hosted and processed on servers in the United States. In addition, ClubRunner employees are located in Canada and other countries outside of the European Economic Area.

ClubRunner may never use the Protected Data for the purposes of advertising third-party content, and will not sell the Protected Data to any third party except as part of a merger or acquisition.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period
ClubRunner retain the personal data provided by the Controller only for as long as it is needed to provide the Services set out in the Agreement. In termination of the Service Agreement or this Data Processing Agreement all the data shall be returned to the Controller or deleted within 90 days, depending on the instructions from the Controller.

ClubRunner may keep personal data to allow us to resolve disputes, enforce our agreements, comply with legal obligations and/or for other legally permissible purposes.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

ClubRunner's sub-processors provide cloud hosting, email, network support and search functionality services and perform these sub-processing activities in order for ClubRunner to provide the Services to Customer. Personal data will be retained for the period determined by the Controller, including until termination of ClubRunner's agreement with Customer, subject to exceptions allowed by law and under the agreement with Customer. For a list of sub-processors, see Annex III.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13
The data exporter's competent supervisory authority will be determined in accordance with the GDPR.

ANNEX II

TECHNICAL AND ORGANIZATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

When providing the Service the Processor shall apply the following technical and organizational measures:

Use Transport Layer Security (TLS) for encryption in transit and Transparent Data Encryption for encryption at rest for SQL databases where PII is stored. Use Firewall rules and Network security groups to reduce services that can connect to SQL databases.

Use encryption at rest for all data by default stored in tables and storage accounts. Enable transparent data encryption and other security measures as provided by Microsoft Azure infrastructure for encrypting data. Use secured, certified data centre to prevent unauthorized physical access to resources.

Enable infrastructure level security and logging to monitor for any suspicious activity, log any new resources setup, audit all administrator activity to the account, and provide security based notifications and suggestions that are regularly reviewed and implemented.

Perform regular checks for TLS configuration, including checking validity of SSL certificates, settings, and all traffic ensured to be HTTPS. Perform periodic checking of infrastructure configuration of resources, including access levels for end users and rules to access resources.

Any data transfer to sub-processors performed with encrypted protocols and data is only retained in sub-processor for as long as required to process it.

Perform backups of data with point in time restoration of 35 days. Setup storage accounts as geo-redundant to keep a duplicate copy in an alternate data centre.

Grant access to personal data and databases only to personnel that require it to perform troubleshooting and maintenance, and revoke access once no longer needed. Enforce Multi-Factor Authentication for personnel in order to gain access to infrastructure portal.

Authenticate end users to the system using custom logic and access levels with unique login names and password combinations.

Store user data in a centralized manner to minimize duplication and easily searchable in order to make it easily exportable and erasable.

Inquiries regarding user data or requests for deletion must be verified by email address or phone numbers prior to processing. Internally document internal policies and procedures and train relevant personnel on what actions to take for requests by end users or by the controller pertaining to their personal data, including anonymization and deletion.

ANNEX III

LIST OF SUB-PROCESSORS

The controller has authorised the use of the following sub-processors:

ENTITY NAME	APPLICABLE SERVICES	COUNTRY	DESCRIPTION OF PROCESSING
ActiveCampaign	Trial Support and Campaigns	United States	Trial request tracking and follow up emails. Passes names and email addresses as obtained from requesting club.
Atlassian	Software ticketing and internal documentation	United States	Software ticketing and internal documentation for personnel
CloudFlare	Network Service	United States	Network Service for public websites including HTTPS support
DeskPro	Customer support and knowledge base platform	United Kingdom	Customer ticketing and knowledge base platform for end user support. Includes names, email addresses and any details shared during support.
GoDaddy	Email Forwarding & Domain Services	United States	Email forwarding and domain name services
MailJet	Email: Delivery & Statistics	United States	Email delivery and statistics service for all outgoing messages for the platform. Passes first name, last name and email address and retains for 7 days.
Microsoft Azure	Data Storage, Application Infrastructure	United States	Main cloud account including data storage, application infrastructure and services
Sendgrid	Email: Delivery & Statistics	United States	Email delivery and statistics for all outgoing messages for the platform. Passes first name, last name and email address and retains for 7 days.

Data Processor

Signature:

Name: Halle Asterbadi

Title: COO

Date: April 28, 2022

Subscriber

Signature:

Name: ULF ANDERSSON

Title: DISTRICT GOVERNOR 2405

Date: JULY 1, 2024