DATA PROTECTION POLICY

1. Policy Control

1.1 Approval

Author / Policy Lead	Prea Deans – Risk & Compliance Manager		
Live Version No.	3.1		
Policy Sponsor	Simon Hopkins (Director of Finance & Corporate Resources	**Sponsor Approved Date:**	24/01/2023
Organisational Governance Approval Level Required	Risk & Audit Committee (Informed)	**Approval Date:**	
Effective Start Date:	9 Feb 2023	**Next Review Date:**	28 Feb 2025

1.2 **Review History:** record of reviews (irrespective of changes made)

Reviewer Name	Reviewer Role	Review Date
Linda Handley-Wright	Risk & Compliance Manager (ARUK) Original version	2015
John Madill	Compliance Programme Lead Biannual Review	2017
John Madill	Compliance Programme Lead GDPR version	2018
John Madill	Compliance Programme Lead Post-GDPR check	01/2019
John Madill/Sandro Scordo – Draft	Governance, Risk and Compliance Lead/Head of Data Biannual Review	12/2020
Prea Deans	Risk and Compliance Manager	18/01/2023
Chris Brown	Data Governance Manager	19/01/2023
Stuart Miller	Head of Governance Assurance & Legal	19/01/2023
Tony Regan	Head of Data & Digital Development	26/01/2023

1.3 **Version History:** record of policy versions and changes made

Version No.	Description of change	Date of Issue
1	Original Version (ARUK)	2015

2	GDPR Version	11/6/2018
3.0 (draft)	New template/ changes to role owners	8/1/21
3.1	Update following RAC Comments	19/4/2021

For generic questions or concerns relating to this or any other policies at VA email policies@versusarthritis.org.

2. Policy Statement

What is data protection law?

Data protection law gives living natural people (also known as Data Subjects) the right to control how their 'personal data' (any information that can be used to identify them, such as name, email address, location data, home address, identification card number, etc.) is utilised.

Versus Arthritis (VA) respects the data and privacy of supporters, service users, staff and volunteers and takes its responsibility to ensure personal data is used in accordance with the law seriously. The charity is committed to complying with all relevant data protection laws, rules and regulations and concedes that no one is exempt from complying.

When processing personal data VA considers:

1) What personal data is needed to manage a relationship or activity. This limits the data collected and stored to either:
    a. The minimum time needed
    b. Data that is only provided by the data subject on their own accord
2) The appropriate and lawful basis for data processing.VA relies on consent only when necessary. We also respect individual preferences by making opt outs easy and clear to see.

Notes:

- The interim Data Protection Officer (DPO) for VA is Tony Regan (T.Regan@versusarthritis.org).
- The deputy DPO for VA is Prea Deans (P.Deans@versusarthritis.org).

3. Lawful bases for processing of Personal Data

There are six lawful bases for collecting personal data. Some of the key lawful bases which VA relies on to collect data are listed below.

1. Consent

Where we collect data from an individual directly, we ensure we obtain valid consent and ensure the purpose for consent to use personal data is specific, clear and easy to withdraw. We may use affirmative action such as tick-boxes or signing a consent statement to do this.

If a person has given third-party consent to share their data with an organisation that acts as a processor, we treat the consent as consent to only share the data with that third party for the purposes clearly specified.

In applying Privacy and Electronic Communications Regulations we group marketing purposes under a single consent. We obtain “opt-in” consent for email, SMS and telephone marketing and make it easy for the data subject to withdraw consent immediately if they wish. Our marketing message is always clear, for a specific purpose and informed.

VA has identified 12 marketing purposes within our charity, which are mapped from our consent webpages to our internal record keeping platform. These include the name of the marketing purpose and a description of it as follows:

Name of Purpose	**Purpose Use**
1) Corporate Fundraising: Information for Trusts	Contacting Trust representatives counts as marketing unless we have a direct relationship. We therefore use this purpose to manage opt-outs and opt ins for relevant Trust contacts.
2) Events: General Events Marketing	This purpose is used for opting in people who are interested in events (sports and community), but not other types of marketing.
3) Fundraising: Appeals	General fundraising activities purpose. (*This purpose was originally to allow for an opt-out of special appeals but we now don't use special appeals so its use was repurposed).*
4) Gambling / Gaming: Raffle	This purpose is used to fulfil the legal requirement to allow people to opt out of receiving gambling promotions and information (e.g. raffles).
5) News (Including Products, Newsletters, Literature): Awareness-raising Campaigns	This purpose is used to opt in supporters interested in news and information regarding the charities recognition and lobbying work, but not interested in other fundraising communications.
6) News (Including Products, Newsletters, Literature): Newsletters	Supporters are opted into this purpose for general organisational news so if they aren't interested in other fundraising marketing they can still hear updates and information about the charity.
7) Professional Engagement: Educational Products	Used as specific opt in to the Healthcare Professional Network. These communications are specific to health professionals so not of interest to the general public.
8) Services: Regular Arthritis information	Individuals with arthritis or those who support people with arthritis are opt into this mailing list on advice for how to live with arthritis.
9) Services: Services Marketing Comms	Allows us to contact people about the services we offer to help people with arthritis. Used as an opt in if they do have an interest and an opt out for people who don't.
10) Trading Company: Trading Company Marketing Comms	*Versus Arthritis Trading Limited* is a wholly-owned trading subsidiary company of the VA charity, which sells Christmas cards and other products and is a separate legal entity. We are required to manage opt-ins and opt-outs for this entity separately.
11) Volunteering: Information for established volunteers	Volunteers may wish to have multiple communications / relationships with the charity. This purpose allows us to manage channel preference for these volunteers.

12) Research: Newsletter	Used as specific opt in to VA's Research newsletter. These communications mainly go to active researchers in the charity (details held on our Grant Tracker platform), but the general public can also opt in to receive research information and news.

We ensure that correct marketing purposes are being applied when we ask for consent and endeavour to regularly review processing activities against these purposes.

2. Legitimate interest

VA uses a balancing test to determine whether legitimate interest can be used as a lawful basis for processing personal data. Two questions are asked as follows:

1) Is the processing of personal data essential for the organisation to function (or could another less intrusive way be used)?
2) Does the processing of personal data outweigh any risk of harm to or the freedom of rights of the data subject?

VA also considers the reasonable expectation of data subjects as to how data may be used by the charity.

We may rely on legitimate interest for postal marketing where relevant to a customer relationship or journey. We always give a prompt to opt out of receiving postal marketing.

3. Performance of a Contract

VA relies upon performance of a contract as a lawful basis where the processing of data is important (if not essential) to perform or enter a contract with the individual data subject(s).

VA only uses this if there is a clear connection between the processing of data and the contract entered by the data subject. For example, an individual may request to join a physical health activity organised by VA. VA needs to process specific data to prepare the individual for the activity facilitated by VA, such as to ensure the individual is fit and healthy to partake in the activity and the activity provider is aware of any health issues the individual may have for health and safety purposes.

4. Vital Interest

In very rare situations, VA may need to process personal data to save someone's life or protect them from serious harm. It is mostly required in situations of emergency medical care.

5. Legal Requirement

VA commonly relies upon this lawful basis when it needs to comply with a statutory obligation. For example, VA may process personal data to comply with its legal obligation to disclose employee salary details to HMRC, as set out in the HMRC website; or to an appropriate Regulator or Court.

4. Retention and disposal of personal data

Personal data is only retained where VA has an organisational or legal need to do so. When VA disposes of personal data if it is no longer needed, it is done in a secure manner. The law and some regulations or contractual agreements may require VA to retain data for a specific time and it may

also be important to keep certain personal data for legal claims or manage an ongoing business relationship.

Data Protection Retention Schedule

Purpose for Retaining Data	Time Limit
Specified retention period is defined in law (e.g. audit requirements).	As specified by relevant legislation.
Managing current relationships (including event participation, volunteers, major donors)	Duration of event activity or relationship plus 6 months, or until consent withdrawn *NB: for core record (including evidence of participation) this will be superseded by the corporate memory purpose.*
Corporate memory: Keeping records of past contact to facilitate future contact	Removal/anonymization/archiving at 10 years after the most recent active contact. **In practice this becomes the overriding retention policy for personally-identifiable data.**
Identifying and recognising our highest-value supporters (those with 8 or more active engagements, those who give an aggregate donation value of £500, branch volunteers with more than 1 year's active involvement)	Indefinite
Legacy pledgers	Indefinite
Trusts	Indefinite
Responding to enquiries	2 years for low-engaged people who have not been converted to supporters.
Administration of wills and legacies	Information about wills and legacies may contain personal data which will be maintained for 10 years. VA notes that a data subject must be a living natural person, and a legator that is deceased therefore is not considered a data subject (and does not fall under GDPR). Nevertheless, we endeavour to apply strict security measures in all situations concerning personal data.
Research	Until grant funding expires

More detailed retention dates are also defined with the assistance of Data Owners and Stewards and recorded with the charities Record of Processing Activity

5. Subject Access Request (communications about Data Processing)

VA has a legal obligation to reply to queries and complaints made by individuals about the personal data we hold about them. We acknowledge the importance of the rights of individuals to access, correct, erase or object to use of their personal data by VA, within a reasonable time.

6. Special Category

Common examples of special category data include any information revealing an individual's race, ethnicity, political stance, religion, trade union membership, genetic data, health or sexual orientation.

As the above types of personal data are very sensitive, VA only uses them (1) where completely necessary and (2) where the suggested collection is thoroughly considered with the lawful basis of explicit consent used. Only very exceptional circumstances allow VA to hold special category data about an individual without their explicit consent, for example, where the data is needed about an individual's health in connection with employment with us.

7. Child Consent

As there are greater risks around sending marketing to children, VA acknowledges the greater level of protection afforded to children under data protection law. In the UK only children aged 13 or over can provide valid consent. VA's guiding principle is to obtain consent from parents if the child is under the age of 18 as an extra precaution. Reasonable efforts are made to verify that the person giving consent is either the parent/guardian (if the child is below 18) or verify their age if they are 18 or over.

8. Training

VA requires all staff and lead volunteers to receive comprehensive GDPR training. VA facilitates a workshop, which is a mandatory requirement to attend. This is to ensure anyone associated with VA that handles personal data is fully equipped and informed before handling it.

9. Record of processing activities

VA acknowledges that the creation of Record of Processing Activity (RoPA) is a legal requirement under GDPR. VA has initiated steps to implement RoPA with the aim of having a formal, documented, comprehensive and accurate record of processing activities, which is reviewed regularly.

VA's RoPA contains the following information:

- Where the data is stored if out of the EEA
- Name of data controller and/or data processor
- Types of data collected
- Lawful basis for collecting data

- An information asset register, which informs VA where data is stored and assigns responsibilities. This also allows us to assure the data has appropriate security measures.

10. Enforcement action

Supervisory Authorities are typically national bodies that enforce the GDPR in EU member states and beyond. The Information Commissioner's Office (ICO) is the competent Supervisory Authority in the UK that VA must report to if a data breach occurs. The ICO has powers to serve notices on us, investigate our operations and, ultimately and for serious breaches, to issue fines for non-compliance.

SCOPE

This policy and its associated procedures and guidance apply to:

- all employees of VA, whether permanent or temporary, casual and agency staff and volunteers when working in or directly for the Charity (Staff);
- all external members of the VA Board of Trustees when acting in that capacity (Trustees);
- all other persons when working in or directly for VA, such as external members of Committees, consultants and contractors (External Representatives).
- Members of branches, groups and other volunteers operating on behalf of VA.

Key terms and definitions

Personal Data: Information either identifying a living individual or that can be linked to such information.

GDPR: General Data Protection Regulation. Former EU law implemented in the UK through the Data Protection Act 2018 – "GDPR" is often used interchangeably with "Data Protection Act 2018"

Consent: An explicit statement or act that indicates a person has asked VA to process data in a particular way.

Purpose: The reason for processing data. A single purpose may encompass a range of activities, e.g. communication, evaluation

Marketing/Direct Marketing: Information provided to a customer or supporter describing the work of VA or encouraging an individual to enter into or extend a relationship (e.g. donation, volunteering).

PECR: Privacy and Electronic Communications Regulations 2003 – requires consent for email and SMS Marketing.

Legitimate interest: A term describing when the charity may process data without consent and in the absence of a contract, vital (safety) interest or legal duty.

ICO: The Information Commissioner's Office (ICO) is an executive non-departmental public body, sponsored by the UK Department for Digital, Culture, Media & Sport. It upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

11. Rationale

This policy sets out the principles by which VA collects and uses personal data. Abiding by data protection legislation allows us to protect our supporters, staff, volunteers and other people's rights. It is vital to the integrity and reputation of VA and allows us to run a better business.

Personal data must be processed in accordance with data protection law. This is primarily the Data Protection Act 2018, the Privacy and Electronic Communications (EC Directive) Regulations 2003 and subsequent amendments, the Payment Card Industry's Data Security Standards and the Computer Misuse Act 1990. Other rules including the Fundraising Code of Practice, the Fundraising Preference Service and Gambling Act 2005 affect how we use personal data. The ICO takes enforcement action against serious infringement and issues guidance and best practice that set the example to follow.

The National Council for Voluntary Organisations (NCVO) set suggested standards for charities to maintain in protecting the privacy of their supporters, while both the Information Commissioners Office and Fundraising Regulator provide comprehensive guidance.

Important note: Breach of this policy and its associated procedures and guidance may constitute a disciplinary offence for employees. Others will be subject to investigation and may be referred to appropriate authorities.

12. Making it Happen

We maintain a set of data protection procedures governing specific activities.

We maintain an organisational privacy notice at www.versusarthritis.org/privacy. Changes to the privacy notice to include new data processing activities are covered under the procedures. More specific privacy information is incorporated into terms and conditions of different activities and services.

We aim to rectify inaccurate personal data as soon as we become aware and take proactive steps to maintain data accuracy. Where we have no obligation to retain inaccurate data, we will erase it.

We have technical and organisational measures in place to ensure appropriate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

We respect the fundamental rights of data subjects in respect of:

- access to data
- rights to request information
- rights to withdraw consent, restrict or object to processing, to rectify inaccuracies and to be forgotten

We offer training and make information available to all employees. We provide guidance and support to volunteers to abide by this data protection policy

We only partner with suppliers that legally commit to follow our data protection standards to process data and we give clear instructions.

We review and revise this policy every 2 years or more frequently if necessary.

We are committed to continuous improvement in management and control of data and data processing, and this is being achieved through implementation of a data strategy.

Appendix:

Data Protection Procedures

VA Privacy Notice

GDPR (EU text, English language)

Data Protection Act 2018

Privacy and Electronic Communications Regulations 2003

Information Commissioner's Office