VFAN Data Privacy Policy – Our Supporters

May 2018

Contents

What data we hold and why?

We hold the names and email addresses of VFAN supporters and records of any donations they have made. VFAN sends a periodic newsletter to supporters who have opted in to receive it and have approved VFAN holding their email address in our database. Supporters who have opted in have been provided with details of how to opt out at any time.

We will only use your information within VFAN for the purposes for which it was obtained. VFAN will not, under any circumstances, share or sell your personal data with any third party for their own marketing purposes, and you will not receive marketing from any other companies, charities or other organisations as a result of giving your details to us. We do not collect or hold "sensitive personal data" about our supporters such as health status.

You may give us your information indirectly when you contribute to VFAN via fundraising sites like Just Giving. These independent 3rd parties will pass your data to us where you have indicated that you wish to support VFAN and in addition, have either given your consent for us to hold your data or it is a necessary part of completing a contract with you.

Who is responsible for processing the data?

Only VFAN employees and contractors have access to the data that we hold on VFAN supporters. All of these individuals sign contracts which incorporate adherence to VFAN's data privacy policy.

How do we ensure data is protected?

We ensure that there are appropriate technical controls in place to protect your personal details. For example, our network is protected and monitored.

We have physical controls in place to ensure that your personal details are not inadvertently shared. For example, an office "clear desk policy" and storing of data in locked cabinets.

How is data stored?

Supporters' data is stored in VFAN's database which can only be accessed by VFAN staff members.

How long does the organisation keep data?

We will hold your personal information on our systems for as long as is necessary for the relevant activity, for example we will keep a record of donations subject to Gift Aid for at least seven years to comply with HMRC rules.

If you request that we stop sending you marketing materials we will keep a record of your contact details and appropriate information to enable us to comply with your request not to be contacted by us.

Where you contribute material to us, e.g. in response to a particular campaign we will only keep your content for as long as is reasonably required for the purpose(s) for which it was submitted unless otherwise stated at the point of generation.

How do we deal with a Subject Access Request?

Under the Data Protection Act you have the right to request a copy of the personal information we hold about you and to have any inaccuracies corrected. Where you, as a VFAN supporter would like to review the data that we hold for you, please make a request to: contact@vfanf.org or send a request in the post to: 27 Old Gloucester Street, London, WC1N 3AX. We will provide the information within 28 days.

To whom does VFAN disclose data?

VFAN currently only discloses supporters' data within the organization.

The only circumstances where VFAN will share your data with 3rd parties, is in order to comply with legal requests where disclosure is required or permitted by law (for example to government bodies for tax purposes or law enforcement agencies for the prevention and detection of crime, subject to such bodies providing us with a relevant request in writing).

If any other circumstance arises where it is necessary for VFAN to share supporters' data, we will always ensure that the 3rd party is fully compliant with GDPR regulations.

Who is responsible for reporting a data breach?

Where there has a potential or actual data breach, this is reported to the Chief Executive Officer who will determine whether there has been an actual breach that needs to be reported to the Information Commissioners Office (ICO) and the individual.

The Chief Executive Officer is ultimately responsible for determining whether there has been a breach and what reporting requirements are subsequently necessary.