Scope of Policy:

Associates
Board members
Volunteers
Staff
Sub-contractors

Data Protection Policy

Public Voice CIC (known here as 'we', 'us', Public Voice or Public Voice CIC) retains and uses personal data (information that relates to and identifies living people) to help us listen to the voices of all service users in order to build powerful evidence. We take, or support others to take, action to deliver positive change in service delivery. Public Voice is a Community Interest Company (CIC) with a mission to improve services through user engagement. We do this through community engagement, individual user engagement and community intervention, collecting the combined voices of services users, gathering evidence and ultimately taking action to bring about positive change, now and in the future. We collect personal information from visitors to our website, through the use of online forms and every time individuals email us their details. We also collect feedback and views from people about the public services they access, including health and care, and the neighbourhoods where they live. In addition, we receive information about our own staff and people who apply to work for Public Voice. We may collect name, email address, phone number, details of feedback or enquiry, demographic details, and further details about staff.

Scope of Policy

This policy sets out how Public Voice meets legal and good practice standards for the protection of personal data (belonging to residents, service users, employees, associates, volunteers or others) and how it expects to apply those standards to those working for Public Voice or handling data on our behalf.

Associated Legislation and Guidance

Data Protection Act (DPA) 2018
General Data Protection Regulation (GDPR) including DPA 2018, Information Commissioner's Office, Information Commissioner's Office

Contents

1. The data protection regime

1.1 The EU-wide General Data Protection Regulation (GDPR) sets standards and sanctions in the case of non-compliance. It has been transposed into the UK by the Data Protection Act (DPA) 2018 and is the basis upon which organisations manage the protection of personal data (also referred to as the 'data subject'). The introduction of the EU-wide General Data Protection Regulation (GDPR) sets new standards and increased sanctions in the case of non-compliance. The Data Protection Act (DPA) 2018, amongst other things, provides further detail on how some of the GDPR provisions are to be enacted in the UK.

1.2 The legislation takes account of the impact of technological changes on privacy and security, to ensure that the individual has control over the personal data that organisations hold on them; and imposes greater uniformity and consistency in the way organisations go about protecting that data.

1.3 We as data controller (responsible for determining the purpose for which data is processed and its protection) take steps to ensure that individuals are able to access and check the accuracy of the data we hold on them, and if incorrect, are able to ask for the inaccuracies to be rectified. Public Voice has put in place processes to ensure that data subject's requests to exercise their rights can be met. The processes enable a data subject to ask for their personal data to be sent to them for their own use, raise objections to the processing of their personal data (e.g. if it is not being used for its stated purpose), or restrict how it is processed; or they can request that it be deleted (e.g. where there is no compelling reason for its continued processing). Public Voice does not charge for this.

1.4 Public Voice is committed to respecting individual rights, to being open and honest with individuals whose data we hold; to avoid causing harm to individuals by using their personal data fairly and securely and not unlawfully disclosing it; deleting it or in any way modifying it; and to provide training and support for staff and volunteers who handle personal data.

1.5 Specifically, we commit to ensuring compliance with GDPR principles:

1.5.1 Lawfulness, fairness and transparency
1.5.2 Purpose specifications & limitations
1.5.3 Data minimisation
1.5.4 Accuracy
1.5.5 Storage limitations
1.5.6 Integrity and confidentiality (security)
1.5.7 Management & Admin
1.5.8 Accountability

1.6 We only collect personal data for specified reasons, and only that which is adequate, relevant and limited with regards to the purpose of processing it. We are responsible for ensuring that the data is up-to-date, and that it is stored securely, clearly, concisely and in a time-limited way concerned only with fulfilling its purpose.

1.7 Under the GDPR definition of what counts as personal data, Public Voice processes personal data which includes e.g. pseudonymised data, ID numbers, IP addresses and social media 'handles'.

1.8 Existing rights are strengthened and some new rights are introduced:

1.8.1 The right to be informed
1.8.2 The right of access
1.8.3 The right to rectification
1.8.4 The right to erasure
1.8.5 The right to restrict processing
1.8.6 The right to data portability
1.8.7 The right to object
1.8.8 Rights to automated decision-making and profiling

1.9 Public Voice undertakes that any marketing activity it carries out will use our existing data bases which can demonstrate that the data subject has given unambiguous freely given affirmative consent for their personal data to be used in this way. Consent has to be specific and indicate unambiguous agreement from the data subject. Public Voice will not send individuals information without demonstrable consent and Public Voice does not assume consent by default.

1.10 Due to the nature of Public Voice's work, there may be instances in which the requirements of GDPR must be balanced against matters of public interest, national security, in relation to criminal offences, breaches of professional ethical codes, in order to protect the individual concerned or to protect the rights and freedoms of another individual

1.11 In all other instances, Public Voice has taken steps to ensure it can report a breach of the GDPR principles (listed at 1.5) to the Information Commissioner's Office (ICO), within 72 hours of being made aware of them. This process takes account of any risk to the rights and freedoms of data subjects

2 Collecting, processing, storing and transferring data

2.1 Public Voice will only processes information necessary to establish or maintain membership or support; to provide or administer activities for members or those in

regular contact with the organisation; and only keep information while the individual is a member or supporter, or as long as necessary for administration and to meet contractual obligations and statutory requirements.

2.2 Public Voice documents its processing of personal data including details of other data controllers/processors and representatives;. It has identified why it processes personal data and maintains a description of the categories of data processed, how long it keeps such data, with clear explanations for different periods of retention, where relevant. It also maintains documentation setting out the technical/organisational security measures taken to protect the data.

2.3 Public Voice publishes privacy notices to explain who we are, what we want to use individuals' personal data for, and who else (if anybody) will have access to it.

2.4 Public Voice will only share the information with people and organisations necessary to carry out activities (where we have permission to share their information with a third party).

2.5 Personal data will only be transferred by Public Voice where the receiving organisation has the appropriate safeguards in place (e.g. legally enforceable agreement and data protection arrangements such as BCRs, Privacy Shield or other mechanisms accepted by regulatory authorities as being adequate).

3 Our data protection responsibilities

3.1 Public Voice is exempt from registering with ICO as it was established for not-for-profit making purposes. If it makes a profit it is for its own purposes and the profit will not be used to enrich others. We must still meet our obligations under the provisions of GDPR and DPA 2018, to ensure accountability and transparency in our handling of personal data.

3.2 We demonstrate our compliance with the accountability principle by:

3.2.1 Adoption of internal adherence to this data protection policy, staff training, audits of data processing and review of HR policies.

3.2.2 Ensuring the documentation or recording of data processing activities (especially where there is higher risk processing) is maintained

3.2.3 Having our data controller advise us on our obligations as a public authority with regards the law, monitoring compliance including procedures and training (e.g. on breach reporting); and as first point of contact (both for data subjects and supervisory authorities e.g. ICO).

3.2.4 Implementing data protection by design and by default measures e.g. data minimisation, ensuring individuals are able to monitor processing and creating and improving security features.

3.2.5 Carrying out data protection impact assessments (DPIA) where appropriate.

3.3 We ensure that Public Voice conducts periodic information audits to determine what personal data we hold, where we get it from (e.g. online, events, surveys, emails, telephone conversations) and who we share it with, for how long we hold it and how secure it is.

3.4 We periodically review how we seek consent, record and manage it, and will refresh records held of requests for consent to ensure we have evidence to demonstrate Public Voice's GDPR compliance.

3.5 We review our privacy notices to ensure they explain how we satisfy individuals' rights to be informed of the purpose and lawful basis for processing their data (e.g. delivering statutory function or contract), and how to contact the data controller.

3.6 We only hold personal data if it is relevant and non-excessive and we only use it for the originally intended purpose.

3.7 If higher risk processing (i.e. where there is a potential risk to the rights and freedoms of individuals, or else involving special categories of data or relating to offences/convictions) or health, biometric or genetic data is planned, we will conduct a DPIA.

3.8 We employ, as required by GDPR, governance measures and good practice tools to conduct privacy impact assessments (PIA) as part of our broader privacy by design approach; building data protection into all our systems, contracts and projects, to ensure personal data is protected[1]. This policy will be complemented where necessary, as part of a wider review of our data protection arrangements (both technical and organisational), with procedures that help us to continue to protect individuals' personal data and comply with the legal requirements.

4. Preventing and acting on data breaches

4.1 A data breach is a failure of security leading to unauthorised access, disclosure, destruction, alteration to, or loss of, data subjects' personal data, whether it be inadvertent or malicious.

[1] See ICO Code of Practice and Article 29 Working Party Guidance

4.2 To safeguard against breaches, we regularly carry out checks on employees handling personal data. We also have structured data governance so that only those that have a need to interact with personal data do so. All data access is strictly controlled by appropriate account access

4.3 We ensure firewalls are secure, malware detection software installed as appropriate, and review and run network security health checks.

4.4 We use strong passwords – with upper and lower case letters, numbers and symbols – to protect the personal data we hold; and encrypted databases with multi-level password access that is frequently changed.

4.5 We also encrypt any portable devices (e.g. laptops, memory sticks, tablets) that are used to store personal information.

4.6 If, as a consequence of a personal data breach, the rights and freedoms of individuals are thought to be at risk (e.g. potentially incurring a financial loss or compromising their confidentiality), Public Voice will notify supervisory authority within 72 hours of being made aware of it.

4.7 We will submit a breach notification including its nature; the categories, estimate of individuals, or records affected; the name and contact details of data protection officer; likely consequences of the breach for the data subjects; and the measures taken, or to be taken, to address it.

4.8 If the risk is high, then we will also notify the affected individuals.