VDT DATA COLLECTION & HANDLING POLICY: 2022 – 2026

This policy should be considered in conjunction with VDT's Data Sharing Policy 2022 – 2026.

Policy written: 2018
Last reviewed: July 2022

VIRGIN TERRITORY Engagement, The Place 2016

WHAT DOES VDT USE DATA FOR?

- For collaborators & staff: to ensure their eligibility to work for us, and to pay them
- For audiences: to contact them (with their consent), sending promotional, marketing information, inviting them to support VDT's work and to anonymously input their data into Audience Finder to build a clear picture of our audience demographics and segmentation
- For funders: to report on company make up, company activity and SMART objectives in line with VDT's major funding agreements
- For venues: to contact them about prospective work, and past tours
- For research: for example, recording interviews for use as creative stimulus in the making process

WHAT DATA DOES VDT COLLECT?

AUDIENCE & PARTICIPANT DATA

Arguably our largest source of data, VDT collects this through several means:

- Ticket sales/Box Office data from venues who have booked us, where data sharing agreements exist (See Data Sharing Policy for more details)
- Audience Finder data from sample audiences at our productions/installations (this data is collected via paper forms/booklets, Google Forms). This data is anonymous but helps VDT to build a clear picture of who our audience is, including our audience demographics and segmentation
- Data collected through participation activity evaluation forms plus registers with participant names/pseudonyms for H&S purposes
- Data collected through YouTube analytics, Google analytics and analytics available through VDT's social media platforms about who is engaging with VDT's work/content

'MARKETING' DATA

- Mailing list, administered through MailChimp and VDT's CRM system SalesForce.

For the purposes of this policy, on stage and on film audiences will be the primary focus.

VDT also collects names and email addresses when audience members opt in to sign up to VDT's newsletter, either through VDT's secure website form or via a physical paper sign-up sheet at tour venues (the physical sheet is later destroyed once the email addresses are added to MailChimp- VDT's GDPR compliant Marketing platform).

VENUE DATA

- Contacts at past venues who have booked VDT and potential future venues. This data is collected through past correspondence, enquiring at the venue via phone or freely available on venue websites.

Data is stored in VDT's CRM system SalesForce, securely in VDT's filing system on SharePoint, or in secure Outlook address books.

STAFF/COLLABORATORS DATA

- VDT collects data about the people we work with for legal/HR purposes

DATA HANDLING

In May 2018 a new General Data Protection Regulation ("the GDPR") changed the way personal data such as HR records and customer lists had to be dealt with. Since then the UK's withdrawal from the EU has meant that a "UK GDPR" (the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019) had to be introduced to ensure that these principles were enshrined in UK law. The key points of these regulations are set out below.

As a data controller and processor, VDT does the following to ensure the company is compliant with UK GDPR:

- Ensures that all subscribers to VDT's newsletter provide unambiguous consent (i.e. written consent; or ticking a box on a web page; or choosing technical settings in an app; or any other statement/conduct that clearly indicates (in this context) the data subject's acceptance of the proposed processing of personal data). Individuals can subscribe to VDT's newsletter either through:
    - Online form via VDT's safe and secure website
    - Physical paper sign-up sheet at tour venues (The physical sign-up sheet will be dated and scanned. The digital version will then be stored securely in the same central place on VDT's SharePoint to act as lasting proof of consent. They will then be manually uploaded into the mailing list database via Mailchimp. The physical copy will be shredded)
    - Written consent via email

For venue contact data which is freely available on websites:

- This process does not apply as the data is being used solely to send relevant information about VDT work with a view to bringing the work to their venue, or inviting to a VDT premiere
- Unless they give specific consent, they are not added to VDT's mailing list

SENSITIVE DATA

Paper copies of contracts etc (addresses, DoB, NI numbers) should be kept in lockable files within the VDT office/Senior Finance Managers office. For cloud-based data, these files should be additionally secured through a password system, in a private folder on SharePoint or stored in VDT's password protected CRM system SharePoint.

This will apply to:

- VDT Confidential logins
- Private HR files, including information on settlements/redundancies etc
- Next of kin contacts for current staff
- Job applications (see below)
- Annual Submission personal data (see below)

ACE ANNUAL SUBMISSION

VDT asks all freelancers, staff and board members to self-identify relevant information about protected characteristics including age, gender, sexuality and ethnicity as per Arts Council England Annual Submission reporting requests, and will continue to use a robust method of ensuring this data is managed securely.

Staff and Freelance data is collected through an anonymous Google Form (the responses are deleted once the data has been submitted to ACE). Board data is collected via a Trustee Word Document as part of the Board induction process, the document asks for the Trustee's consent for VDT to keep hold of the data for future years reporting (VDT retains this information securely via SharePoint). Any emails containing personal information are deleted.

The above process is explained to all parties before any information is requested.

All hard-copies of sensitive data when no longer required will be securely shredded and destroyed, and not processed through our usual paper recycling method.

TIMELINE FOR DELETION/SHREDDING OF SENSITIVE DATA:

- Child licence information (daily logs, sign in/out sheets etc): 6 months after last date on the licence (with the exception of the licence application itself, for future reference)
- Job applications: 1 year after application
- Financial records information: 6 years after the finish of the pertaining financial year

- Past employees (sensitive information e.g. next of kin): Upon completion of contract. Other information (i.e. contracts, contact information) will remain on file.

PARTICIPANTS/COLLABORATORS FROM SENSITIVE BACKGROUNDS

The proposed areas of work moving forward for the company will involve discussion and thereby collection of data from members of the population including women at risk of domestic violence, refugees, adoptive parents and their children and young people.

With the exception of children, all of these groups will be afforded additional safeguarding measures in relation to their data in the following ways:

- Liaison with gatekeepers in collaborative organisations; drawing upon their best practice in relation to storing data
- Ensuring pseudonyms are used in relation to storing any sensitive information/testimonies gathered in research period
- Keeping a secure file of pseudonyms / real names for internal reference only
- For any of these groups for whom a contract may be raised, to follow the above guidelines for their cloud and physical storage

For children, we will ensure we have parental/guardian consent for collection of data for children, evidenced through contracts & email correspondence.

This policy will be reviewed biennially or more frequently if recommended/required, and will be included in all staff inductions.

RIGHT TO ACCESS, CHANGE, CORRECT DATA & WITHDRAW CONSENT

The UK GDPR includes the right to withdraw consent to data processing. All collaborators and participants must be informed of the following before they give any consent to data processing:

- Their right to request access to their personal information
- Their right to request correction of their personal information
- Their right to request that we correct the personal information we hold about you, although we may need to verify the accuracy of the new information you provide to us
- Their right to request erasure of their personal information
- Their right to object the processing of their personal information
- Their right to request restriction of processing their personal information
- Their right to request transfer of their personal information

- Their right to withdraw consent

VDT will aim to respond to all legitimate requests within one month.

TRANSFERRING DATA TO THE EU & OTHER COUNTRIES

It has long been the case that data can only be transferred to other countries that offer "adequate protection", i.e. have data protection legislation at least as rigorous as the country of origin. This is taken as a given within the European Economic Area (the EU plus Norway, Iceland and Liechtenstein), as long as the processing meet all the rest of the GDPR requirements. Transfers to other countries are also unrestricted where an 'adequacy' decision has been made. That means that recipient country has been judged to have a data protection regime that provides at least the same level of protection to personal data as there is in the sending country.

After a period of uncertainty, the EU has made a full adequacy decision for the UK, which will be reviewed in 2025.

The EU also has adequacy decisions in respect of Andorra, Argentina, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Switzerland and Uruguay. In addition, adequacy decisions have been made for Canada (in respect of transfers to commercial organisations only) and Japan (for transfers to non-governmental organisations only). The UK has adopted all these adequacy decisions, with the addition of Gibraltar, and including all the EEA countries. This means that transfers from the UK to the EU and these other countries are unrestricted.