Visual Language Professionals Ltd

GENERAL DATA PROTECTION REGULATION (GDPR) POLICY

Policy Approved By The Management Committee On: ***17 February 2018***

Policy Became Operational On: ***01 March 2018***

1. Definitions

- 'VLP' – Visual Language Professionals Ltd.
- 'EU' – European Union.
- 'GDPR' – General Data Protection Regulation.
- 'Processing' – the obtaining, recording, storing, updating and sharing of information.

2. Background

2.1. On 25 May 2018, the EU General Data Protection Regulation (GDPR), Regulation (EU) 2016/679, replaces the Data Protection Directive 95/46/EC. The GDPR was designed to harmonise data privacy laws across Europe, to protect and empower all EU citizens' data privacy and to reshape the way organisations across the region approach data privacy.

3. Scope, Implementation And Review

3.1. This policy is created for use by VLP only and should be used to inform procedure and decision-making.

3.2. VLP has conducted a review of its Data Protection Policy and procedures to ensure that it is compliant with the EU GDPR before members are invited to renew their membership with VLP on, or before, 01 April 2018.

3.2.1. Implementation of this policy will ensure that personal data supplied by members and held by VLP will be processed only for the purposes for which it was provided.

3.2.2. The implementation and annual review of this policy is designed to comply with the EU GDPR; information will be processed and shared with external third-parties only as Contracted and Consented (see Section 4); personal data will be held securely to minimise the risks associated with data breaches; and, data will be safeguarded from physical and electronic theft.

3.2.3. VLP wishes to remain transparent with all members about how it processes personal data. VLP believes that the best way to secure against data breaches is to implement and regularly review its EU GDPR Policy.

3.3. This policy is expected to remain in operation until the law governing it is superseded; however, it will be reviewed on an annual basis or as procedure concerning processing of personal data dictates, whichever is sooner.

3.4. This policy will be assigned a date and version number, which will be displayed in the document footer and updated each time the policy is revised or updated.

3.4.1. All updates and revisions shall be approved by the Management Committee.

3.5. The Management Committee will instigate and collate a data audit annually in February (see Section 7.7). It is expected that the data audit will involve all members of the Management Committee. The completed audit will be held securely along with all other VLP documentation (see Section 7.3).

3.5.1. The data audit will document all personal data held, where it comes from and how it is processed. The aim is to identify all personal data that VLP processes and how it flows into, through and out of the organisation.

3.6. Members are invited to raise any concerns about personal data or the VLP GDPR Policy by emailing admin@vlp.org.uk. Concerns will be brought to the attention of the Management Committee for discussion and action, where required.

4. Lawful Basis

4.1. VLP relies on two lawful bases for collecting data; Contract and Consent.

4.2. In contracting with members, VLP must necessarily collect, process and store members' personal data to provide them with the services that they have asked VLP to provide them with; these are VLP's Core Services.

4.2.1. Article 6(1)(b) of the GDPR states that there is a lawful basis for processing information where "processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract".

4.2.2. On joining and at annual renewal of membership, members contract with VLP to provide Core Services. These are;

1) membership of an organisation representing professional workers with D/deaf people, including those who have retired or are taking time out of the profession, and where member records are held on a member database; and,
2) that they be introduced to professional indemnity insurance (PII), which is currently provided by McParland Finn Ltd (trading as MFL Professional) and the insurers Barbican Protect Limited (on behalf of certain underwriters at Lloyd's under Binding Authority No: B0775UEB32617). This will only apply where a member has confirmed that they would like to include professional indemnity insurance as part of their membership and has paid the associated premium. Information will be shared between VLP and the insurer.

4.2.2.1. Where a member does not wish to include professional indemnity insurance as part of their membership and/or does not pay the additional premium, their personal data will not be shared with McParland Finn Ltd (trading as MFL Professional) and the insurers Barbican Protect Limited (on behalf of certain underwriters at Lloyd's under Binding Authority No: B0775UEB32617).

4.2.3. Without processing members' personal data, VLP and its Management Committee would not be able to administer a membership organisation, nor would it be able to introduce members to professional indemnity insurance provided by McParland Finn Ltd (Trading as MFL Professional).

4.3. In addition to the VLP Core Services, members can consent to their data being shared in order to be provided with VLP's Additional Services.

4.3.1. On joining and at annual membership renewal, members will be given the option of consenting to their personal information being processed;

- for membership communications;
- by external partners (see Section 7);
- and displayed on the VLP website and VLP App; and,
- for statistical purposes.

4.3.2. On completion of joining and annual membership renewal, members will be emailed a copy of the consents that they have given.

4.3.3. Members will be asked to confirm that they understand that they may, at any time, withdraw their consent to any, or all, of the consents that they have given. Members will be provided with the email address membership@vlp.org.uk to send withdrawal of consent notifications (see Section 5).

4.3.4. Where a member withholds a consent, they will be emailed by the Management Committee or other nominated officer explaining how the withholding of a particular consent will impact on the services they receive as members and inviting them to review the consents that they have given.

5. Member Rights Concerning Personal Data

5.1. Members have a right to know how their personal data is being processed and who VLP is sharing their data with.

5.1.1. Members will be required to read and declare that they have understood a privacy statement, before completing a membership application and on annual membership renewal.

5.2. Members have the right to;

- obtain confirmation that their data is being processed;
- access their personal data and other supplementary information;
- data rectification and data quality; and/or,
- request that their personal data be erased.

5.2.1. For all requests relating to the rights mentioned in Section 5.2, members are required to email membership@vlp.org.uk and requests will be actioned without delay and within one (1) calendar month.

5.2.2. The identity of the requester will be verified before any information is supplied and identity verification will take the form of an email reply asking the requester to supply all of the following;

- First name and surname.
- House number and postcode.
- Last three digits of the mobile telephone number VLP holds.
- VLP membership number.

5.2.2.1. Where the member request relates to data inaccuracy of verification data, the other three pieces of data will be used for verification and the inaccurate information matched with VLP's own records.

5.2.2.2. Where inaccurate personal data has been provided to third-party data-processors, all appropriate steps will be taken to inform the third party of the data rectification required.

5.2.3. Requests for information received by email will only be responded to by email.

5.3. Members' have a right to request erasure of personal data when;

- it is no longer necessary in relation to the purpose for which it was originally collected and processed.
- the individual withdraws consent.
- the individual objects to processing and there is no overriding legitimate interest for continuing the processing.
- it was unlawfully processed (in breach of GDPR).
- erasure will comply with a legal obligation.
- it is processed in relation to the offer of information society services to a child.

5.3.1. VLP can refuse to erase personal data;

- to exercise the right of freedom of expression and information.
- to comply with a legal obligation for the performance of a public interest task or exercise of official duty
- for reasons of public health in the public interest
- for archiving purposes in the public interest, scientific research, historical research or statistical purposes.
- for the exercise or defence of legal claims.

5.3.2. A request for personal data erasure will be reviewed by the Management Committee or other nominated officer.

5.3.3. Where it is decided that personal data must be erased, the member will be notified by the Management Committee or other nominated officer 72 hours in advance of their data being irretrievably deleted and giving the member the option of changing their mind by sending a return email to the Management Committee asking that their information be retained.

5.4. Members have the right to request that the information VLP hold about them is supplied for the purposes of data portability.

5.4.1. Where a member requests access to this information, it will be supplied without delay and within one (1) calendar month.

5.4.2. The identity of the requester will be verified in accordance with Section 5.2.2.

5.4.3. The information will be provided by email free of charge in a commonly used machine-readable format.

6. Use Of Third-Parties

6.1. VLP uses carefully selected third-parties to provide services and where these are used, a written contract is in place so that both parties understand their responsibilities and liabilities.

6.2. VLP is responsible and liable for ensuring that third-parties comply with the GDPR and will only appoint processors who can provide guarantees that the requirements of the GDPR will be met and the rights of data subjects protected.

6.3. Third-party suppliers will be provided with the Chair's email address for reporting any data breaches that they experience that involves the destruction, loss, alteration, unauthorised disclosure of, or access to, personal information of VLP members.

7. Data Security

7.1. VLP will provide all members of the Management Committee with a dedicated email address for the sole use of VLP activities.

7.1.1. To safeguard against accidental data breaches when sending emails, the address of the intended recipient shall be checked prior to sending.

7.1.2. Any group email to members shall ensure that the Bcc (blind carbon copy) function is used to safeguard against a data breach and protect against the disclosure of members' email addresses.

7.2. Members' personal data will be held electronically on the VLP Google Drive.

7.2.1. Members' personal data will only be accessed by members of the Management Committee and other nominated officers to carry out necessary processing duties in relation to VLP's Core Services offered by membership and the Additional Services that members have consented to.

7.2.2. All personal data held electronically will be backed-up on the last working day of each month.

7.3. All physical VLP business correspondence, documentation and financial information will be kept by the Management Committee in a locked filing cabinet.

7.4. All members of the Management Committee who use a digital device/workstation to access any VLP information or emails will ensure that that device/workstation is password protected at all times and will lock the device/workstation if they walk away from it.

7.5. Where VLP uses a third-party to process payments, no record of members' payment details is retained.

7.5.1. Members may make payment by cheque or direct bank transfer and financial records of such transactions will be held securely in accordance with section 7.3.

7.5.2. Any financial payments that need to be made or refunded to members will be made by cheque and sent to the named member at the address provided when joining or at annual renewal. Where a direct funds transfer is used, the member will need to provide their account number and sort code and these details will be held securely in accordance with section 7.3.

7.6. All detected data breaches will be notified to the Chair, who will investigate and keep a record of all reported breaches. This information shall be discussed with the Management Committee to review current procedures and make recommendations for amendments, if required.

7.6.1. Individual members will be informed of a data breach if the breach is likely to result in a high risk to their rights and freedoms.

7.7. A data audit (see Section 3.5) shall be held annually, unless required sooner, and discussed with the Management Committee to ensure that any issues are identified, rectified and communicated.

8. Information Commissioner's Office (ICO) Registration

8.1. Every data controller who is processing personal data is required to register with the ICO, unless they are exempt.

8.1.1. VLP believes that it is exempt from registering with the ICO because it was established for not-for-profit making purposes and any profit is for its own purposes and is not used to enrich others. Under these guidelines, VLP will only process;

- information necessary to establish or maintain membership or support;
- necessary to provide or administer activities for people who are members of the organisation or have regular contact with it;
- with people and organisations necessary to carry out the organisation's activities, if members give permission to share their information;
- and keep the information while the individual is a member or supporter or as long as necessary for member administration.

9. International Data Transfers

9.1. VLP operates in the United Kingdom (England, Scotland, Wales and Northern Ireland) and personal data will not be transferred outside of these borders, internationally.

10. Compliance And Risk

10.1. The Management Committee or other nominated officer shall keep a documented record of all issues and member requests related to the VLP GDPR policy and this will be presented to the Chair annually.

10.2. Any member of the Management Committee can highlight identified personal data risks to the Chair, by email. The Chair will be responsible for coordinating procedures to mitigate identified risks and for logging and risk assessing information assets.

10.2.1. An action plan will take appropriate action to terminate or mitigate risks that are not tolerated.

10.3. VLP shall consider and embed data protection by design and by default into all new processing activities.

10.3.1. A Data Protection Impact Assessment (DPIA) shall be undertaken when using new technology or when processing is likely to result in a high risk to the rights and freedoms of individuals.

10.4. The role of Data Protection Officer (DPO) will be undertaken by the Chair and any issues regarding personal data or a breach involving the unauthorised disclosure of, or access to personal data, will be reported to the Chair.