LIQUID FRIDAY
Building a better workforce world.

Liquid Friday
Data Retention Policy

1. Introduction

This Policy sets out the type(s) of personal data held by the Company for employment and payroll purposes, including personal data received from or shared with recruitment agencies, hirers, end-clients and other organisations involved in placing, engaging or managing workers, the period(s) for which that personal data is to be retained, the criteria for establishing and reviewing such period(s), and when and how it is to be deleted or otherwise disposed of. For further information on other aspects of data protection and compliance with the DPA, please refer to the Company's Data Protection Policy.

The DPA defines "personal data" as any information relating to an identified or identifiable natural person (a "data subject"). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

The DPA also addresses "special category" personal data (also known as "sensitive" personal data). Such data includes, but is not necessarily limited to, data concerning the data subject's race, ethnicity, politics, religion, trade union membership, genetics, biometrics (if used for ID purposes), health, sex life, or sexual orientation.

Under the DPA, personal data shall be kept in a form which permits the identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. In certain cases, personal data may be stored for longer periods where that data is to be processed for archiving purposes that are in the public interest, for scientific or historical research, or for statistical purposes (subject to the implementation of the appropriate technical and organisational measures required by the DPA to protect that data).

In addition, the DPA includes the right to erasure or "the right to be forgotten". Data subjects have the right to have their personal data erased (and to prevent the processing of that personal data) in the following circumstances:

a) Where the personal data is no longer required for the purpose for which it was originally collected or processed (see above);
b) When the data subject withdraws their consent;
c) When the data subject objects to the processing of their personal data and the Company has no overriding legitimate interest;
d) When the personal data is processed unlawfully (i.e. in breach of the DPA);
e) When the personal data has to be erased to comply with a legal obligation;

This Policy sets out the type(s) of personal data held by the Company for employment and payroll purposes, the period(s) for which that personal data is to be retained, the criteria for establishing and reviewing such period(s), and when and how it is to be deleted or otherwise disposed of. For further information on other aspects of data protection and compliance with the DPA, please refer to the Company's Data Protection

Policy.

2. Aims and Objectives

2.1 The primary aim of this Policy is to set out limits for the retention of personal data and to ensure that those limits, as well as further data subject rights to erasure, are complied with. By extension, this Policy aims to ensure that the Company complies fully with its obligations and the rights of data subjects under the DPA.

2.2 In addition to safeguarding the rights of data subjects under the DPA, by ensuring that excessive amounts of data are not retained by the Company, this Policy also aims to improve the speed and efficiency of managing data.

3. Scope

3.1 This Policy applies to all personal data held by the Company including personal data relating to employees, workers, contractors, agency workers, candidates and other individuals whose personal data is processed in connection with the Company's recruitment, payroll, employment, work-finding or workforce management activities.

Personal data, as held by the Company is stored in the following ways and in the following locations:

3.1.1 The Company's servers, located in Portsmouth, United Kingdom
3.1.2 Third-party servers, operated by Salesforce.com and located in London, UK.
3.1.3 Computers permanently located in the Company's premises at 3-6 The Quarterdeck, The Boardwalk, Port Solent, PO6 4TP
3.1.4 Laptop computers and other mobile devices provided by the Company to its employees;
3.1.5 Physical records stored in 3-6 The Quarterdeck, The Boardwalk, Port Solent, PO6 4TP
3.1.6 Archived paper records in OASIS Group, Winchester, Hampshire, UK
3.1.7 Contract E-Signing software servers, operated by Congasign and located in the EU
3.1.8 SMS solution operated by smsmagic.com and located in the EU
3.1.9 Online Application operated by FormAssembly based in the US, but servers are located in the EU.
3.1.10 Head office HR records and Holiday Pay operated by PeopleHR, located in the EU.

3.2.11 Personal data received from or shared with recruitment agencies, employment businesses, hirers, end-clients and other organisations with which workers are placed or engaged, including information necessary for recruitment, onboarding, work allocation, payroll, compliance, right-to-work checks, workforce management and the administration of the working relationship.

4. Data Subject Rights and Data Integrity

All personal data held by the Company is held in accordance with the requirements of the DPA and data subjects' rights thereunder, as set out in the Company's Data Protection Policy.

4.1 Data subjects are kept fully informed of their rights, of what personal data the Company holds about them, how that personal data is used and with whom it may be shared, as set out in Parts 12 and 13 of the Company's Data Protection Policy, and how long the Company will hold that personal data (or, if no fixed retention period can be determined, the criteria by which the retention of the data will be determined).

4.2 Data subjects are given control over their personal data held by the Company including the right to have incorrect data rectified, the right to request that their personal data be deleted or otherwise disposed of (notwithstanding the retention periods otherwise set by this Data Retention Policy), the right to restrict the Company's use of their personal data, the right to data portability, and further rights relating to automated decision-making and profiling, as set out in Parts 14 to 20 of the Company's Data Protection Policy.

5. Technical and Organisational Data Security Measures

5.1 The following technical measures are in place within the Company to protect the security of personal data. Please refer to Parts 22 to 26 of the Company's Data Protection Policy for further details:

5.1.1 All emails containing personal data must be encrypted;

5.1.2 All emails containing personal data must be marked "confidential";

5.1.3 Personal data may only be transmitted over secure networks;

5.1.4 Personal data may not be transmitted over a wireless network if there is a reasonable wired alternative;

5.1.5 Personal data contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely. The email itself and associated temporary files should be deleted;

5.1.6 Where personal data is to be sent by facsimile transmission the recipient should be informed in advance and should be waiting to receive it;

5.1.7 Where personal data is to be transferred in hardcopy form it should be passed directly to the recipient or sent using secure recorded mail via Royal Mail Recorded Delivery; and

5.1.8 All personal data transferred physically should be transferred in a suitable container marked "confidential";

5.1.9 No personal data may be shared informally. Where access to personal data is required, access shall only be provided where there is a legitimate business or legal need and in accordance with the Company's Data Protection Policy and applicable access controls.

5.1.10 All hardcopies of personal data, along with any electronic copies stored on physical media should be stored securely;

5.1.11 Personal data may be shared with employees, agents, contractors, recruitment agencies, employment businesses, hirers, end-clients,

payroll providers, pension providers, professional advisers, IT service providers, public authorities and other third parties where there is a lawful basis for doing so and where the sharing is necessary for the relevant business, employment, recruitment, payroll, compliance or workforce management purpose. Such sharing shall be carried out in accordance with the Company's Data Protection Policy and applicable data protection legislation.

5.1.12 Personal data must be handled with care at all times and should not be left unattended or on view;

5.1.13 Computers used to view personal data must always be locked before being left unattended;

5.1.14 No personal data should be stored on any mobile device, whether such device belongs to the Company or otherwise without the formal written approval of Data Protection Officers and then strictly in accordance with all instructions and limitations described at the time the approval is given, and for no longer than is absolutely necessary**;**

5.1.15 No personal data should be transferred to any device personally belonging to an employee and personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of the Company where the party in question has agreed to comply fully with the Company's Data Protection Policy and the DPA;

5.1.16 All personal data stored electronically should be backed up every 24 hours with backups stored onsite and offsite. All backups should be encrypted;

5.1.17 All electronic copies of personal data should be stored securely using passwords and encryption;

5.1.18 All passwords used to protect personal data should be changed regularly and should must be secure;

5.1.19 Under no circumstances should any passwords be written down or shared. If a password is forgotten, it must be reset using the applicable method. IT staff do not have access to passwords;

5.1.20 All software should be kept up-to-date. Security-related updates should be installed as soon as reasonably possible after becoming available;

5.1.21 No software may be installed on any Company-owned computer or device without approval; and

5.1.22 Where personal data held by the Company is used for marketing purposes, it shall be the responsibility of Marketing Executive or Data Protection Officer to ensure that the appropriate consent is obtained and that no data subjects have opted out, whether directly or via a third-party service such as the TPS.

5.2 The following organisational measures are in place within the Company to protect the security of personal data. Please refer to Part 27 of the Company's Data Protection Policy for further details:

a) All employees and other parties working on behalf of the Company shall be made fully aware of both their individual responsibilities and the Company's

responsibilities under the DPA and under the Company's Data Protection Policy;

b) Only employees and other parties working on behalf of the Company that need access to, and use of, personal data in order to perform their work shall have access to personal data held by the Company. Where personal data is shared with recruitment agencies, employment businesses, hirers, end-clients or other third parties, access shall be limited to the information reasonably necessary for the relevant purpose;

c) All employees and other parties working on behalf of the Company handling personal data will be appropriately trained to do so;

d) All employees and other parties working on behalf of the Company handling personal data will be appropriately supervised;

e) All employees and other parties working on behalf of the Company handling personal data should exercise care and caution when discussing any work relating to personal data at all times;

f) Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed;

g) The performance of those employees and other parties working on behalf of the Company handling personal data shall be regularly evaluated and reviewed;

h) All employees and other parties working on behalf of the Company handling personal data will be bound by contract to comply with the DPA and the Company's Data Protection Policy;

i) All agents, contractors, or other parties working on behalf of the Company handling personal data must ensure that any and all relevant employees are held to the same conditions as those relevant employees of the Company arising out of the DPA and the Company's Data Protection Policy;

j) Where any agent, contractor or other party working on behalf of the Company handling personal data fails in their obligations under the DPA and/or the Company's Data Protection Policy, that party shall indemnify and hold harmless the Company against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

k) Where the Company shares personal data with recruitment agencies, employment businesses, hirers, end-clients or other third parties, the Company shall ensure that the sharing is carried out on a lawful basis, that only relevant and necessary information is shared, and that appropriate contractual, technical and organisational safeguards are in place where required.

6. Data Disposal

Upon the expiry of the data retention periods set out below in Part 7 of this Policy, or when a data subject exercises their right to have their personal data erased, personal data shall be deleted, destroyed, or otherwise disposed of as follows:

6.1 Personal data stored electronically (including any and all backups thereof) shall be deleted securely using the industry recognised secure deletion standards.

6.2 Special category personal data stored electronically (including any and all backups thereof) shall be deleted securely using the industry recognised secure deletion standards.

Liquid Friday Ltd | Company No: 588 7477 | VAT Reg No: 889 8562 35
3-6 The Quarterdeck, The Boardwalk, Port Solent, PO6 4TP

6.3 Data stored in hardcopy form shall be shredded to at least EWC 20 01 01 standards;

7. Data Retention

7.1 As stated above, and as required by law, the Company shall not retain any personal data for any longer than is necessary in light of the purpose(s) for which that data is collected, held, and processed.

7.2 Where personal data is obtained during registration, recruitment or onboarding but no employment, worker, contractor or other relevant relationship is confirmed or commenced, the Company will normally retain that personal data for no more than six months, unless a longer period is required or permitted by law, or the individual has provided consent for their details to be retained for future recruitment or work opportunities.

7.3 The applicable data retention period will normally commence from the end of the relevant contract, worker, contractor or other contractual relationship, or from the date on which the relevant processing activity or recruitment process ends, as applicable. Where a specific statutory or regulatory retention period applies, that period will take precedence.

7.4 Different types of personal data, used for different purposes, will necessarily be retained for different periods **(**and its retention periodically reviewed), as set out below.

7.5 When establishing and/or reviewing retention periods, the following shall be taken into account:

7.5.1 The objectives and requirements of the Company;

7.5.2 The type of personal data in question;

7.5.3 The purpose(s) for which the data in question is collected, held, and processed;

7.5.4 The Company's legal basis for collecting, holding, and processing that data;

7.5.5 The category or categories of data subject to whom the data relates;

7.6 If a precise retention period cannot be fixed for a particular type of data, criteria shall be established by which the retention of the data will be determined, thereby ensuring that the data in question, and the retention of that data, can be regularly reviewed against those criteria.

7.7 Notwithstanding the following defined retention periods, certain personal data may be deleted or otherwise disposed of prior to the expiry of its defined retention period where a decision is made within the Company to do so (whether in response to a request by a data subject or otherwise).

7.8 In limited circumstances, it may also be necessary to retain personal data for longer periods where such retention is for archiving purposes that are in the public interest, for scientific or historical research purposes, or for statistical purposes. All such retention will be subject to the implementation of appropriate technical and organisational measures to protect the rights and freedoms of data subjects, as required by the DPA.

Liquid Friday Ltd | Company No: 588 7477 | VAT Reg No: 889 8562 35
3-6 The Quarterdeck, The Boardwalk, Port Solent, PO6 4TP

Type of Data	Purpose of Data	Review Period	Retention Period or Criteria	Comments
Full Name	Identify Data Subject & RTI with HMRC	Annual	10 years	Used to identify customer on CRM and HMRC for Payroll Purposes
Date of Birth	Identify Data Subject & RTI with HMRC	Never	10 Years	Used to identify customer on CRM and HMRC for Payroll Purposes
Age	Identify Data Subject & RTI with HMRC	Never	10 Years	Used to identify customer on CRM and HMRC for Payroll Purposes
Gender	RTI with HMRC	Never	10 Years	Used to identify for HMRC for Payroll Purposes
National Insurance No.	Identify Data Subject & RTI with HMRC	Never	7 Years	Used to identify customer on CRM and HMRC for Payroll Purposes
UTR Number	Ensure correct deduction of CIS for HMRC	Never	7 Years	Used for HMRC for Payroll Purposes
Nationality	Track and monitor Right to Work	Annual/ Expiry of document	10 Years	Used to confirm Right To Work
Visa Details	Track and monitor Right to Work	Annual/ Expiry of document	Duration of employment plus 2 years	Used to confirm Right To Work
VAT Registration	Ensure correct deduction of VAT for HMRC	Never	7 Years	Used for HMRC for Payroll Purposes
Student Loan Status	Ensure correct deduction for HMRC	Never	7 Years	Used for HMRC for Payroll Purposes
Mobile Number	Identify & Contact Data Subject	Annual	Duration of employment plus 2 years	Used to identify customer on CRM
Home Telephone	Identify & Contact Data Subject	Annual	Duration of employment plus 2 years	Used to identify customer on CRM
Email Address	Identify & Contact Data Subject	Annual	Duration of employment plus	Used to identify customer on CRM

			2 years	
Address	Identify & Contact Data Subject	Annual	10 Years	Used to identify customer on CRM
Next of Kin Name	Emergency Contact Details	Annual	End of Contract	Used to contact if an emergency at work.
Next of Kin Contact	Emergency Contact Details	Annual	End of Contract	Used to contact if an emergency at work.
Next of Kin Relationship	Emergency Contact Details	Annual	End of Contract	Used to contact if an emergency at work.
Sort Code	Payment of wages	Annual	Duration of employment plus 6 years	Used for payment of wages
Account Number	Payment of wages	Annual	Duration of employment plus 6 years	Used for payment of wages
Building Society No.	Payment of wages	Annual	Duration of employment plus 6 years	Used for payment of wages
Account Name	Payment of wages	Annual	Duration of employment plus 6 years	Used for payment of wages
Security Question Answer	Secure data subject account	Never	End of Contract	Used for ensuring Data Protection and identity
Security Password	Secure data subject account	Never	End of Contract	Used for ensuring Data Protection and identity
Court/ CMEC Deduction Orders	Ensure correct deduction for HMRC	Annual	7 Years	Used for HMRC for Payroll Purposes
SSP Details	Ensure correct payment of SSP	Annual	7 Years	Used for HMRC for Payroll Purposes
MATB1	Maternity details to ensure correct payment of SSP	Annual	7 Years	Used for HMRC for Payroll Purposes

Passport	Track and monitor Right to Work	Annual/ Expiry of document	Duration of employment plus 2 years	Used to confirm Right To Work

Liquid Friday Ltd | Company No: 588 7477 | VAT Reg No: 889 8562 35
3-6 The Quarterdeck, The Boardwalk, Port Solent, PO6 4TP

8. Roles and Responsibilities

8.1 The Company's Data Protection Officers are Jake Kingshott, Sarah Jones and Harrison Bridger 02392 88300 or DPO@liquidfriday.co.uk.

8.2 The Data Protection Officers shall be responsible for overseeing the implementation of this Policy and for monitoring compliance with this Policy, the Company's other Data Protection-related policies (including, but not limited to, its Data Protection Policy), and with the DPA and other applicable data protection legislation.

8.3 The Data Protection Officers shall be directly responsible for ensuring compliance with the above data retention periods throughout the Company.

8.4 Any questions regarding this Policy, the retention of personal data, or any other aspect of DPA compliance should be referred to the Data Protection Officer.

9. Implementation of Policy

This Policy shall be deemed effective as of March 2026. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

This Policy has been approved and authorised by:

Name:	Jade McDonald
Position:	People Specialist
Due for Review by:	Oct 2027