LetHQ LTD Data Retention Policy

Introduction

The need to retain data varies widely with the type of data held by LetHQ. Some data can be immediately deleted while other data may need to be retained into the future. This policy seeks to describe the company's policy for specific data retention and deletion.
The scope of this policy covers all company data stored on LetHQ-owned, company-leased, and otherwise company-provided systems and media.

Regulation

LetHQ is required to comply with the General Data Protection Regulation 2016 (GDPR), the Data Protection Act 2018 and the Data Protection (Amendment) Act 2003. In August 2017, the Government passed the Data Protection Bill which will bring the GDPR into UK law. There are some instances, however, where other legislation and regulations will supersede the GDPR and these are detailed below.
In the event of a data loss, destruction or transmission, LetHQ will be obliged to report this to the individual or company affected, as well as the Information Commissioner's Office (ICO) which has power to impose a financial penalty for a breach up to €20 million or 4% of worldwide turnover. There is a mandatory requirement to report the breach to the individual and to the ICO within 72 hours of LetHQ becoming aware of it.
The ICO has advised that all UK businesses will need to comply with GDPR despite Brexit. This is because it will affect all data subjects in Europe or carrying out processing of data in Europe or about European data subjects.

Reasons for Data Retention

It is not practical or cost-effective to save all data. Some data must be retained to protect LetHQ's interests, preserve evidence and audit trails, while generally conforming to good business practices. Reasons for data retention include:

- Litigation.
- Accident Investigation.
- Security Incident Investigation.
- Regulatory requirements.
- HMRC requirements.
- Intellectual property preservation.

As data storage increases in size and decreases in costs, companies often err on the side of storing data in several places on the IT network. A common example of this is where a single file may be stored on a local user's machine, on a central file server, and on back-up system.

When identifying and classifying LetHQ's data it is important to understand where that data is stored, particularly for duplicate copies, so that this policy may be applied to all duplicates of the information.

Data Retention Requirements

This section sets out the agreed guidelines for retaining the different types of company data that are held by LetHQ:

- Client data will be held for as long as the organisation remains a client of LetHQ, plus 6 years.
- Website enquiry data will be held for 6 months.
- Applicants' consent data and details entered by the applicant and referees will be kept for 12 months.
- VAT records will be held for 6 years.
- Security Incident Reports will be held for 3 years.
- Health & Safety records will be retained for 3 years.
- Supporting documents are deleted or destroyed once they have served their purpose under GDPR.

If any data retained under this policy is stored in an encrypted format, consideration must be given for secure storage of the encryption keys. Encryption keys must be retained as long as the data the keys decrypt is retained. Reference to Vigo IT Solutions, our IT provider, should be made if there is any doubt as to how data should be encrypted, and keys retained.

Data Destruction

Data destruction is a critical part of the data retention policy. Data destruction ensures that LetHQ uses data efficiently thereby making data management and data retrieval more cost effective. There are good reasons to delete data after a reasonable amount of time. These include the following:

- It is easier to keep more limited amounts of data secure.
- It is easier to find specific data in a response to a Subject Access Request, or when searching data for other purposes.
- It is consistent under GDPR to securely delete data that is no longer required for its original purpose.
- If it is retained for a long period, it is more likely to be inaccurate and out of date.

When the above timeframe expires, company staff must actively destroy the data covered by this policy. If a user feels that certain data should not be destroyed, they should identify the data to their line manager so that an exception to the policy can be considered. Exceptions may only be approved by the Managing Director of LetHQ.

At present there is no automated facility by which emails, and files can be automatically destroyed. It will be necessary to carry out these tasks manually. Consideration should be given to mapping data flows in a Data Privacy Impact Assessment (DPIA) to identify the different locations and format of data held.

If security is not maintained and there is a data loss, the fact that excessive data has been retained, and therefore put at risk, is a factor which the ICO can take into account when considering whether to impose a civil penalty and the level of that penalty. The breach is more likely to be regarded as serious if no old data has ever been deleted, if there is no data retention policy, or if no thought has been given to whether old data should be deleted.

LetHQ specifically directs users not to destroy data in violation of this policy. Destroying data that a user may feel is harmful to themselves is expressly forbidden, as is destroying data in an attempt to cover up a violation of law or company policy.

Enforcement

This policy will be enforced by the Manager Director of LetHQ. Violations will result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of company property (physical or intellectual) are suspected, the company may report such activities to the applicable authorities.