Policy status

This policy was adopted by the Company on 14th July 2020 and last reviewed 24th September 2021

Scope

The aim of this policy is to ensure that procedures are in place and are being implemented to ensure that personal data we hold is controlled, used appropriately, stored securely and that those whose data we hold have full control over this. Statlog Pro Limited has a corporate responsibility to ensure that it conforms to and implements the GDPR.

The implementation of this policy ensures that we are fully complaint with the General Data Protection Regulation (GDPR); effective from 28 May 2018.

This policy applies to all personal data for which Statlog Pro Limited is responsible, including electronic data and manual data which are covered by the GDPR.

Responsibilities

All staff and suppliers or contractors who work with Statlog Pro Limited and who have access to personal information for which Statlog Pro Limited is responsible, will be expected to comply with this policy and with the GDPR.

Statlog Pro Limited are accountable to the Information Commissioner for its compliance with the legislation.

Any breach of the policy may result in Statlog Pro Limited, as the registered data controller, being liable in law for the consequences of the breach. Legal liability may also extend to the individual processing the data and their Mangers, under certain circumstances. In addition, breach of this Data Protection Policy by staff will be considered to be a disciplinary offence and will be dealt with according to Statlog Pro Limited disciplinary procedures.

What is personal data?

The GDPR applies to 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.

What personal data do we obtain / hold?

We generally only hold a small amount of personal data in respect of clients, suppliers, contractors, and others. We hold slightly more data for our employees. We only ever hold adequate and relevant data, limited to what is necessary to operate our business effectively and for no other purpose.

We do not hold or process 'sensitive data' under the scope of the GDPR

We have undertaken a review of data use within our current business and have concluded that a data protection impact assessment (DPIA) is not required and that the data or processing of that data is not considered 'high risk' under the scope of the GDPR. When new avenues of business are undertaken / explored, the need for a DPIA is formally reviewed.

The following is all the personal data we would currently ever hold: -

In respect of Statlog Pro Limited employees, clients, potential clients, suppliers, consultants, contractors, collaborating organisations and officials: -

- Names
- Business addresses
- Business telephone numbers
- Business email addresses
- Personal addresses (if individuals have given this to us)
- Personal telephone numbers (if individuals have given this to us)
- Personal email addresses (if individuals have given this to us)

In respect of potential Statlog Pro Limited employees: -

- CVs and job application forms
- Interview notes
- DBS checks

In respect of Statlog Pro Limited employees: -

- CVs and job application forms
- NI numbers, PAYE tax references and HMRC RTI payroll reference
- DBS checks
- DBS check numbers and whether satisfactory or unsatisfactory
- Date of birth
- Next of kin name and contact telephone number
- Driving licence details
- Motor insurance details
- Passport numbers
- Bank account details (sort code and account number)
- Employment record including appraisals, disciplinary record etc
- Pensions scheme details (personal scheme reference number)

What are the risks?

Most, if not all, of the personal data we process in respect of clients, potential clients, suppliers, consultants, contractors, collaborating organisations and officials is already freely available within the public domain. The likelihood of any harm resulting in a data breach of this information is very low.

Some employee personal data is more sensitive and could be used for eg identification fraud.

What is the lawful basis applicable to us for processing personal data?

Consent: the individual has given clear consent for us to process their personal data for a specific purpose. This applies to almost all the personal data we process in respect of Statlog Pro Limited employees, clients, potential clients, suppliers, consultants, contractors, collaborating organisations and officials. Explicit consent is obtained via the procedures outlined within this policy.

Contract: the processing is necessary for a contract we have with the individual, or because they have asked us to take specific steps before entering into a contract. This applies to Statlog Pro Limited employees, and also project specific data relating to clients, potential clients, suppliers, consultants, contractors and collaborating organisations and officials, and also to our facilities service term contracts.

Legal obligation: the processing is necessary for us to comply with the law (not including contractual obligations). This would apply to much of the data we process in respect of eg our employees, but also to other personal data we hold and our duty to comply with all aspects of the law as it relates to our business.

Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. This would apply to Statlog Pro Limited employees, project specific data relating to clients, potential clients, suppliers, consultants, contractors and collaborating organisations and officials.

Why do we hold personal data?

Because we need this to carry out our business, and

Because an individual has consented to be on one of our databases, or

Because we have worked with an individual in the normal course of our business, or

Because an individual is or has been an employee of Statlog Pro Limited

How do we use personal data?

In order to contact the individual or their organisation, or

In the case of our contractor or supplier databases, in order to contact an individual or organisation and to allow others to contact them in respect of their business and services, or

In the case of employees to manage their employment and payroll, and in the case of emergencies

In the case of employees, names and career history on our website and within marketing material

In the case of clients and potential clients, for occasional direct marketing from Statlog Pro Limited

Who do we share personal data with?

With our staff, clients, potential clients, suppliers, consultants, contractors, collaborating organisations and officials in the context of our day to day business with the individual, and

In the case of our contractor, consultants or supplier databases, in order to allow database users (both inside and outside our organisation) to search for, select and contact an individual in respect of their business and services, or

Also in the case of employees we share the more sensitive personal data only with Statlog Pro Limited Partners and HR staff, with HMRC, the Statlog Pro Limited pension provider, the Statlog Pro Limited pensions advisor, the Statlog Pro Limited medical insurance company and (non-sensitive information) with future employers who have requested an employment reference

How do we obtain consent to hold, store or use personal data?

Where explicit consent is required to hold, store or use an individual's personal data, we obtain this consent in the following ways and store this consent for future reference: -

- Via our database consent form / privacy notice, or
- In the case of our contractor or supplier databases, via our database questionnaire / privacy notice
- In the case of employees, via their contracts of employment and privacy notice

Where do we keep personal data?

Within databases on our password protected servers

On our website (limited personal data).

Within project specific documents on our password protected servers and within paper files.

Within password protected project archives on our servers, backup devices and within paper files.

Within the Cloud (password protected).

On password protected PC's laptops and mobile phones belonging to the company and used during the normal course of our business.

Sensitive employee information within password secured files on our servers or secure paper files.

How can those we hold personal data about find out what we hold?

An individual can email helpdesk@statlog.co.uk or call us on 03331 123 133. Where a request has been made, the requester will initially be provided with a list of the type of data we hold (not the actual data) via a pro-forma email response within 14 working days. If they then require the actual data, they will be asked to verify their identity before data is sent. All to be made of this procedure so they can advise and enquiring individuals.

How do we keep the personal data secure?

Live and archived data stored within our anti-virus protected servers, PCs and laptops / portable devices, all of which are password / PIN protected and only available to our staff.

Live and archived data stored within the Cloud is encrypted and encryption key protected.

Live paper project files are kept within our secure office, to which only staff have access.

Access to our Cloud based databases is restricted to password protected user accounts with external users heavily restricted in terms of access and permissions.

How long do we keep personal data?

Where this relates to a project or contract, we are legally bound to keep all associated data for a period of twelve years, after which it will be automatically removed and securely destroyed / deleted.

Where this relates to our client, contractor, or supplier databases, until such a time as they tell us they no longer want us to process their personal data. After such a request we retain a certain amount of data (name and contact details) in order to ensure their non-processing request is respected into the future.

Where this relates to an employee, all data (except DBS checks) is kept during the period of employment.

Where this relates to an ex-employee, we are legally bound to keep some data for a period of twelve years after employment. After 12 years all employee data except name and contact details will be automatically and fully deleted.

In respect of employee DBS checks, the actual check in full is only held for long enough to determine satisfactory / unsatisfactory check. The DBS number and whether this is satisfactory or unsatisfactory is held for as long as the employee remains an employee of Statlog Pro Limited and then for a period of 12 years from leaving date.

In respect of potential employee DBS checks, the actual check in full is only held for long enough to determine satisfactory / unsatisfactory check.

In respect of potential employee data (DBS checks), this is held for a 24-month period.

What procedures do we have in place to deal with a data breach?

We have procedures in place to monitor, defend and deal with data breaches as and when they may occur.

Anyone who considers that the Policy has not been followed with respect to personal data about themselves should raise the matter with the Directors at Statlog Pro Limited or email helpdesk@statlog.co.uk.

How can those whose personal date we hold have this permanently and completely deleted?

Everyone has a legal right to 'be forgotten'. An individual can email helpdesk@statlog.co.uk or call us on 03331 123 133. Where a request 'to be forgotten' has been made, the following procedure will be enacted: -

We will advise the individual as to what we can do as follows: -

1. Where the individual is a current employee, we cannot remove relevant data required to enable continued employment.
2. Where the individual is an ex-employee, we can only remove data completely after 12 years from last day of employment. We will, however, remove the individual from our current databases within 14 days verification of request and from our employee archive automatically within 12 years and 28 days of last employment at Statlog Pro Limited.
3. Where the individual has data stored on a project file, this can only be removed 12 years after the completion (Practical Completion) of that project and will be automatically removed from our project archive within 12 years and 28 days of the Practical Completion of the project.
4. Where the individual is on one of our current databases, we will remove all personal data form our current databases within 14 days of request, except name and contact information which will be retained in order to ensure we respect the request not to process their personal data into the future.

We will verify then individuals identify and the request as genuine by utilising the email and / or telephone number we hold for that individual. Providing verification is obtained, we will remove the individual form our current databases within 14 days (name and contact detailed excepted).

Formal review

We formally review the continued adequacy, relevance, and accuracy of all the personal data we hold every five years by reviewing the business and re-issuing privacy notices to all and refreshing consent as follows: -

- Via our database consent form / privacy notice, or
- In the case of our contractor or supplier databases, via our database questionnaire / privacy notice
- In the case of employees, via their contracts of employment and privacy notice

Staff induction and training

In order to ensure that all who work at Statlog Pro Limited understand and respect personal data rights, this policy is provided to all new employees during their induction period. In addition, special training is given to staff who work with our databases and / or (more sensitive) employee information – eg our HR, helpdesk, development and marketing departments.

Regular data protection refresher training is provided to all staff as required.

Signature:

Date: 24th September 2021

Name: Andrew Etherington

Position: Director