Document	Option Software Processing Policy/Agreement
Version	1.0.0
Author	Jamie
Created On	01/06/2022
Modified By	Jamie
Modified On	22/09/2022

About This Policy

This processing policy must be read in conjunction with: Option Software's Privacy Policy/Notice and our Terms and Conditions.

Option Software have legal obligations under the UK GDPR and are subject to regulation by supervisory authorities.

The UK GDPR sets out seven key principles:

- Lawfulness, fairness, and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

These principles should lie at the heart of your approach to processing personal data.

Preamble

This data processing policy/agreement governs the obligations of Option Software and the Client's legal obligations under the Data Protection Act 2018 and the UK's implementation of the General Data Protection Regulation (GDPR).

Index

17. Notification of potential data protection infringements by the client (Data Controller)
18. Transfers of personal data to a third country or an international organisation
19. Access required to Personal Data
20. Consent
21. Effective date
22. If we make any changes to this document

Appendix

1. The Controllers obligations and rights
2. The Processors obligations and rights

Attributions

1. ICO Information Commissioner's Office

1. Definitions and Interpretation

Unless otherwise defined herein, capitalised terms and expressions used in this Agreement shall have the following meanings:

Option Software

The company acting as the Data Processor.

The Client

The company, Individual who signs up to use Option Software's services.

Unless specified otherwise, any references to The Client will refer to:

- *Existing Customers*
- *Past Customers*
- *Potential Customers*

Client Authorized Users

These are the people have been granted access to our products/services by The Client.

They are also going to be one of the Data Subjects, as they will most likely be employees of The Client.

Option Software Services

Option Software provides OneBoxBM as a service (typically called SaaS), this means we deliver applications over the Internet; software as a service.

Subscribers do not have to install any software or update any software Option Software manage everything for you from providing access to the application, security, maintenance, and performance.

Third-party services

Third party service providers are any company, person or entity that performs a service to Option Software.

Option Software pays for the services provided by the third party, a separate company, person or entity.

Subscription Account

A subscription account is an agreement between Option Software and a Client The Client will receive access to Option Software's software services and provide payment for those software services, usually for a one-month period paid in advance of the service being provided.

Data protection law

Option Software and all users of our services must comply with current data protection law when processing personal data.

The GDPR is Europe's new framework for data protection laws. It replaces the previous 1995 data protection directive.

The new regulation started on 25 May 2018. It will be enforced by:

The Information Commissioner's Office (ICO).

What is personal data

Personal Data is information that relates to an identified or identifiable individual.

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/what-is-personal-data/

What is special category data

The UK GDPR defines special category data as:

- Personal data revealing racial or ethnic origin.
- Personal data revealing political opinions.
- Personal data revealing religious or philosophical beliefs.
- Personal data revealing trade union membership.
- Genetic data.
- Biometric data (where used for identification purposes).
- Data concerning health.
- Data concerning a person's sex life; and
- Data concerning a person's sexual orientation.

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/

Data Controller

The Client is the Data Controller and determines the purposes for which and the means by which personal data is processed. So, if your company/organisation decides 'why' and 'how' the personal data should be processed it is the data controller.

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/controllers-and-processors/

Data Processor

The Data Processor processes personal data only on behalf of the Data Controller. The Data Processor is usually a third-party external to the company. However, in the case of groups of undertakings, one undertaking may act as processor for another undertaking.

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/controllers-and-processors/

Sub processor

Means any natural person or legal person, public authority, agency or other body which processes personal data on behalf of appointed by or on behalf of Option Software**.**

Sub processors are by Option Software in order help to process Personal Data on behalf of The Client in connection with an Agreement.

Data Security

Data Security means protecting digital data, such as those in a database, from destructive forces and from the unwanted actions of unauthorized users, such as a cyberattack or a data breach.

Secure Sockets Layer (SSL)

SSL is a protocol for web browsers and servers that allows for the authentication, encryption and decryption of data sent over the Internet.

Transport Layer Security (TLS)

TLS Is a widely adopted security protocol designed to facilitate privacy and data security for communications over the Internet. A primary use case of TLS is encrypting the communication between web applications and servers, such as web browsers loading a website.

A confidentiality agreement

Is a legal agreement that binds one or more parties to non-disclosure of confidential or proprietary information.

2. Introduction

Contracts

- Whenever a controller uses a processor, there must be a written contract (or another legal act) in place.
- The contract is important so that both parties understand their responsibilities and liabilities.
- The UK GDPR sets out what needs to be included in the contract.
- If a processor uses another organisation (ie a sub-processor) to assist in its processing of personal data for a controller, it needs to have a written contract in place with that sub-processor.

3. The subject matter of the processing

Any Personal Data is processed by Option Software on behalf of The Client; all Processing is necessary, proportionate and consistent with our business purpose of providing our software services to the extent permitted by applicable Data Protection Laws.

4. The duration of the processing

Option Software will provide processing services and support to the client for the duration of the contract between us.

5. The nature and purpose of the processing

The majority of the data being processed will be handled by our SaaS solution at the request of the either The Client or one the Client Authorised Users.

The products/services provided by Option Software are intended to be used by The Client and its Authorised Users directly; see below for a breakdown of the responsibilities of each party.

The individuals at Option Software are responsible for:

- The ongoing development and maintenance of the products/services provided by Option Software.
- Testing the products/services, provided by Option Software, to make sure that work as expected and that neither the integrity nor the security of Subject Data is compromised.
- Supporting The Client and The Client Authorised Users while they make use of the products/services provided by Option Software.
- Investigating any issues that arise while The Client and its Authorised users are using the products/services provided by Option Software.

The Client and The Client Authorised Users are responsible for:

- The creation of new data/records
- The viewing of existing data/records
- The editing of existing data/records
- The deleting of existing data/records
- The searching of data/records
- Controlling access to data/records
- The sorting of data/records
- Analysis of the data/records
- The viewing of audit logs relating to data/records
- The viewing of audit logs relating the requests for data/records

(In some cases, this will include personal data.)

The data is processed to allow our Clients and Client Authorized Users to input and manage data of the People engaged in their business.

6. The categories of Data Subject and the type of Personal Data processed

The products/services provided by Option Software are designed/built to evolve to meet the needs of our clients.

This means that scope of the data being processed will increase over time, however the personal data being processed will always fall under certain categories; *see the sub sections below*.

Given the intended purpose of our products/services, which is business management, the data being processed is intended support our clients in managing their business. This includes both helping them:

- Manage their workforce
- Maintain their relationships with 3rd parties

This will include Personal Data of an individual person or multiple people in both a personal and professional capacity.

6.1 Personal Capacity

- Title
    - Mr
    - Mrs
    - Miss
    - Etc.
- Name
    - First and Last
    - First, Middle and Last
- Personal contact details
    - Phone Number
    - Mobile Phone Number
    - Email Address
    - Etc.
- Personal address

6.2 Professional/Work Capacity

- Work contact details
    - Phone Number
    - Mobile Phone Number
    - Email Address
    - Etc.
- Work address
- Employment Details
- Contract Details
- Details of Time Off/Leave/Absence
- Reviews/Feedback/Improvement

6.3 Comments/Notes

Comments/Notes are intended to allow The Client and its Authorised Users to provide extra detail about both the data being processed and the Data Subject as a whole.

This includes, but is not limited to:

- Providing clarification about the data being processed
- Adding extra information that isn't already captured as part of the processing
- Capturing details of meetings or discussions with and/or about the data subject
- Providing feedback about the data subject
- Providing opinions about the data subject

As the comments/notes are what's known as Free Text, it is impossible for Option Software identify the full scope of the data being processed. Therefore, we can only make assumptions based upon the context that our products/services are designed for, which is business management.

In addition to this, individuals at Option Software are not directly responsible for the processing of the Subject Data. This means that we cannot be held in anyway responsible for the content within the comments/notes.

6.4 Documents

The Client and its Authorised Users can attach documents to Data Subjects.

This includes, but is not limited to:

- Identification
- Contracts and Agreements
- Policy Documents
- Training Records

As the content of the documents is unknown to Option Software, it is impossible for Option Software identify the full scope of the data being processed. Therefore, we can only make assumptions based upon the context that our products/services are designed for, which is business management.

In addition to this, individuals at Option Software are not directly responsible for the processing of the Subject Data. This means that we cannot be held in anyway responsible for the content within the attached documents.

7. Controller's Documented Instructions

In order to comply with GDPR regulations, the processor must only act on the controller's documented instructions, unless required by law to act without such instructions.

Signing up to use our services means The Client is instructing Option Software to process Personal Data for them; this makes you (the client) a Data Controller.

Having a subscription-based account will enable our clients and the clients authorised users to input and manage Personal Data about the individuals that are engaged in their business.

Option Software will only process the Personal Data, identified with this document, for the purpose of delivering the company's main services to you, the client.

8. Confidentiality

In order to comply with GDPR regulations, the processor must ensure that people processing the data are subject to a duty of confidence.

Anyone authorised by Option Software to work within our software and services will work on a need-to know' basis. All individuals will have previously committed to a confidentiality agreement.

9. Security Measures

In order to comply with GDPR regulations, the processor must take appropriate measures to ensure the security of processing.

Option Software has measures in place to keep The Clients personal data as secure as possible.

We have internal policies and procedures on information security, including:

- Guidance on maintain a proper work environment, so we can ensure that Personal Data is handled correctly.
- Guidance on making sure that data is backed up correctly.
- Guidance on making sure that data is destroyed correctly regardless of whether it's stored electronically or on paper.
- Guidance on data retention, so we can make sure that we're not keeping data longer that we should be.

We will take all reasonable technical and organisational precautions to protect your personal data from loss, misuse or alteration.

All data you provide is:

- Stored in a password protected environment
- Hidden behind a firewall
- Stored in a virus and malware protected environment

In addition to this:

- We limit and control all user access to our systems
- We limit and control physical access to our building and office
- We enforce a "need to know" policy for access to any data
- We also have a confidentiality agreement in place.
- All data you send to us or receive from us will be encrypted using SSL/TLS technology.

(Any data transmission over the internet is possibly insecure, therefore no one can guarantee 100% security of any data sent over the internet.)

10. Sub-Processors

In order to comply with GDPR regulations, the processor must only engage a sub-processor with the controller's prior authorisation and under a written contract.

Option Software uses a number of third-party services both to process and assist in securing The Clients data.

We have included links in the table below to enable our clients to read about our selected service providers including their GDPR compliance and security measures.

Option Software shall not appoint or disclose any Client or Client Authorised users Personal Data to any Sub-processor unless required to provide our software and services to you or authorised by the Client other than were stated within this document.

Option Software reserves the right to change any third-party service providers at any time at the discretion of the company.

Option Software will ensure that any selected third party used to provide services to us are reputable and fully compliant with current GDPR Regulations, any third parties who have access to The Clients Personal Data will only process it on behalf of Option Software and are obligated not to disclose or use it for any other purpose.

Name:	HostingUk.Net
Description:	HostingUk.Net is responsible for hosting the core part of our products/services. This includes our SaaS solution and its related databases.
Documents:	Data centre: https://hostinguk.net/datacentres Privacy Notice: https://hostinguk.net/terms

Name:	Amazon S3
Description:	Amazon S3 is responsible for hosting The Clients documents using their cloud services.
Documents	Data Storage https://aws.amazon.com/s3/ Privacy Notice https://aws.amazon.com/privacy/?nc1=f_pr

11. Data Subject Access Requests (DSAR)

In order to comply with GDPR regulations, the processor must take appropriate measures to help the controller respond to requests from individuals to exercise their rights.

Under this agreement, Option Software is a data processor for the client.

Option Software cannot fulfil subject access requests for The Clients Authorised Users of our software and services (because the client is the data controller).

If Option Software receives a subject access request directly from a data subject Option Software will direct the Data Subject to their Data Controller, which would be The Client.

Option Software cannot respond to a client's Data Subject access request directly.

Except on the fully documented instructions from the client or as required by any applicable law, Option Software will inform the client prior to providing any information under any legal requirement or any other circumstances.

Option Software will assist the client (the Data Controller) where deemed necessary by providing information and/or documentation if requested by the client to support any request.

Option Software must be given reasonable time to assist with such requests in accordance with Applicable Law.

12. Data Breach

In the event of a data breach Option Software:

- Will without delay notify the client of any suspected or confirmed personal data breach within a 72-hr time limit of the knowledge of such an event.
- Will describe, in clear and plain language, the nature of the personal data breach.
- Will provide the name and contact details of the person managing the breach, where more information can be obtained.
- Will Provide a description of the likely consequences of the personal data breach.
- Will provide a description of the measures we have taken or propose to take to deal with the personal data breach and, where appropriate, a description of the measures taken to mitigate any possible adverse effects.
- Will provide the client with specific and clear advice on any steps they can take to protect themselves.
- Will also notify the client of any possible significant disruption likely to affect their services due to a data breach.

13. End of Contract

In order to comply with GDPR regulations, the processor must delete or return all personal data to the controller (at the controller's choice) at the end of the contract, and the processor must also delete existing personal data unless the law requires its storage.

In the event that you, The Client, no longer wish to use Option Software as a Data Processor. You can request that your account is closed, and that all data we process on your behalf is deleted from our systems.

Alternatively, you can also choose to just cancel your subscription but still keep your account open; *see section 14. Cancellation.*

Upon cancellation Option Software shall provide confirmation, via email, to The Client that it has fully deleted all data within 10 business days of the date of the request; this process is automated, so will normally receive notification, via email, within a few minutes.

While we are able to delete all data we process as The Clients Data Processor, there are exceptions to what we can delete as a Data Controller this includes:

- Data required for our accounting and auditing purposes
- Data relating to The Client and their account, but not data relating to The Clients Data Subjects
- Any communication between Option Software and The Client
- Any communication between Option Software and Client Authorised Users
- Any communication between Option Software and The Clients Data Subjects

(*All of the exceptions listed above are either due to use being required by law or are in the legitimate interests of the business as they are relating to the contract between you and Option Software.)*

In the event that we, Option Software, choose to no longer act as a Data Processor on your behalf we will:

- Notify you of our decision, so you can retrieve your data from our systems.
- Close your account and delete your system data; the data we process on your behalf.

In extreme cases we may close your account without prior notification; this would generally be if we obtained evidence that you or one of your authorised user were using our system to engage in unlawful activity.

14. Cancelation

The Client (the Data Controller) can cancel the subscription to use Option Software's products/services at any time.

Should The Client, choose to cancel your subscription, The Client can do so from within the product/service provided by Option Software.

Any cancellation requests made by The Client will be processed depending upon whether your subscription is either:

1. Due for renewal

The Clients access to the system will be revoked once the process has started.

Or

2. Ongoing

The Client will maintain access to the system for duration in which The Client has paid.

Once The Clients subscription is cancelled you will have the option to either:

1. Leave all data as is; allowing you to start a new subscription in future.
2. Choose to end your contract with us completely; *see section 13. End Of Contract*.

Should The Client decide not to pay the invoice for their subscription renewal, but not actually choose to cancel their subscription. Option Software will treat this subscription has having lapsed, at which point it is effectively cancelled; if your subscription has lapsed and you wish to continue using Option Software as a Data Processor then will need to start a new paid subscription.

15. Duration of Services

Option Software will provide processing services and support to The Client for the duration of the contract between us; this is contingent upon having either an active paid or trial subscription.

16. Audits and Inspections

In order to comply with GDPR regulations, the processor must submit to audits and inspections. The processor must also give the controller whatever information it needs to ensure they are both meeting their article 28 obligations.

Upon request by a Client (the Data Controller), Option Software (the Data Processor) shall make available to The Client all information considered necessary to demonstrate compliance with the contents of this document, and shall allow for and cooperate with an audit, or inspection by The Client or an auditor acting for The Client.

The client shall give reasonable written notice of no less than 30 days to Option Software of any proposed audit or document inspection; any audit or document inspection shall not be conducted more than once in a 12-month period.

Option Software will without undue delay, inform a Client If:

- Option Software receives an inspection by a supervisory authority.
- Option Software receives an inspection by a third party.

17. Notification of potential data protection infringements by the client (Data Controller)

Option Software will notify the client if any of their instructions or requests would lead to a breach of the UK GDPR or local data protection laws.

(*This is on the basis that Option Software are required to do this in order to maintain GDPR compliance.*)

18. Transfers of personal data to a third country or an international organisation

Option Software does not transfer Personal Data to third countries.

Option Software does not transfer Personal Data to any international organisation outside of our listed 3rd party service providers.

19. Access required to Personal Data

At times Option Software will require access to the Personal Data belonging to The Client and its Data Subjects.

Only selected individuals at Option Software will be authorised to access this data; *each individual will have previously committed to a confidentiality agreement.*

See each of the sections below for the circumstances in which such access is required and the reasons for doing so.

19.1 When Providing Support

In order for Option Software to provide support to our clients Option software will on occasions require access to the Personal Data belonging to The Client and its Data Subjects.

When possible, the data will be copied to a controlled test environment so that any issues can be investigated. This will allow Option Software to take the necessary actions to conduct the investigation without risking the integrity of The Client and its Data Subjects Personal Data.

Should the results of an investigation require the data to be restored or corrected then Option Software will either:

- Inform The Client or The Client Authorised User of the changes they need to make to the data.
- Make the changes to the data directly then inform The Client or The Client Authorised user of the changes that have been made; *the data maybe inaccessible to anyone other than Option Software*

Prior to accessing the Personal Data belonging to The Client and its Data Subjects, Option Software will try to resolve any issues using test or dummy data.

Any relation this has to an identifiable person or persons will be purely coincidental asl it will be generated randomly.

19.2 When Maintaining and Upgrading our Systems.

In order for Option Software to maintain and upgrade its systems and its products/services. Option Software will require access to where the Personal Data belonging to The Client and its Data Subjects is stored.

This is due to Option Software needing to make changes to the underlying data structure to support the ongoing development of our products/services.

In order to ensure that we do not compromise the integrity of The Client and its Data Subjects data tests may be carried out both before and after making the changes.

Such tests will always be carried out a copy of the data prior the changes being made to the live environment; *the live environment being the products/services that The Client and their Client Authorised users are accessing.*

19.3 Analysing Personal Data.

In order for Option Software to continue to develop its products/services, it will undertake regular analysis of The Client and its Data Subjects data both Personal and Non-Personal.

Such analysis will be limited to:

- Counting the total number of records and grouping them by various criteria.
- Counting the total number of actions and grouping them by the type of action that has taken place.
- Determining whether or not data is being stored in certain fields.

In each of the above cases the aggregation of the data will be handled by our systems. Individuals at Option Software will not see the underlying data or take part in the aggregation of the data.

20. Consent

By giving consent you are giving Option Software explicit consent to access and process personal data entered into our systems specifically for the purposes identified in this document.

(Consent is obtained by checking the relevant box on our website when accessing our products or services or when communicating with Option Software.)

21. Effective date

This agreement is effective upon registering for access to Option Software's products/services.

The agreement will then be effective until the contract is terminated by either The Client or Option Software.

22. If we make any changes to this document

You will be given 30 days notice If we make any changes to this policy.

Appendix

1. The Controllers obligations and rights

What are your responsibilities as a Data Controller?

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/controllers-and-processors/what-does-it-mean-if-you-are-a-controller/

(The following statements are from the ICO, you can find further information and clarification on the points below on their website.)

If you are a controller

You are responsible for ensuring your processing – including any processing carried out by a processor on your behalf – complies with the UK GDPR.

Your UK GDPR responsibilities include the following:

Compliance with the data protection principles

You must comply with the data protection principles listed in Article 5 of the UK GDPR

Individuals' rights

You must ensure that individuals can exercise their rights regarding their personal data, including the rights of access, rectification, erasure, restriction, data portability, objection and those related to automated decision-making.

Security

You must implement appropriate technical and organisational security measures to ensure the security of personal data.

Choosing an appropriate processor

You can only use a processor that provides sufficient guarantees that they will implement appropriate technical and organisational measures to ensure their processing meets UK GDPR requirements. This means you are responsible for assessing that your processor is competent to process the personal data in line with the UK GDPR's requirements. This assessment should take into account the nature of the processing and the risks to the data subjects.

Processor contracts

You must enter into a binding contract or other legal act with your processors, which must contain a number of compulsory provisions as specified in Article 28(3).

Notification of personal data breaches

You are responsible for notifying personal data breaches to the ICO and, where necessary, other supervisory authorities in the EU, unless the breach is unlikely to result in a risk to the rights and freedoms of individuals. You are also responsible for notifying affected individuals (if the breach is likely to result in a high risk to their rights and freedoms).

Accountability obligations

You must comply with the UK GDPR accountability obligations, such as maintaining records, carrying out data protection impact assessments and appointing a data protection officer.

International transfers

You must comply with the UK GDPR's restrictions on transfers of personal data outside of the UK.

Co-operation with supervisory authorities

You must cooperate with supervisory authorities (such as the ICO) and help them perform their duties.

Data protection fee

You must pay the ICO a data protection fee unless you are exempt.

2. The Processors obligations and rights

What are your responsibilities as a processor?

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/controllers-and-processors/what-does-it-mean-if-you-are-a-processor/#1

(The following statements are from the ICO, you can find further information and clarification on the points below on their website.)
Processors have less autonomy and independence over the data they process, but they do have several direct legal obligations under the UK GDPR and are subject to regulation by supervisory authorities. If you are a processor, you have the following obligations.

Controller's instructions

You can only process the personal data on instructions from a controller (unless otherwise required by law). If you act outside your instructions or process for your own purposes, you will step outside your role as a processor and become a controller for that processing.

Processor contracts

You must enter into a binding contract with the controller. This must contain a number of compulsory provisions, and you must comply with your obligations as a processor under the contract.

Sub-processors

You must not engage another processor (ie a sub-processor) without the controller's prior specific or general written authorisation. If authorisation is given, you must put in place a contract with the sub-processor with terms that offer an equivalent level of protection for the personal data as those in the contract between you and the controller.

Security

You must implement appropriate technical and organisational measures to ensure the security of personal data, including protecting against accidental or unlawful destruction or loss, alteration, unauthorised disclosure or access.

Notification of personal data breaches

If you become aware of a personal data breach, you must notify the relevant controller without undue delay. Most controllers will expect to be notified immediately, and may contractually require this, as they only have a limited time in which to notify the supervisory authority (such as the ICO). You must also assist the controller in complying with its obligations regarding personal data breaches.

Notification of potential data protection infringements:

You must notify the controller immediately if any of their instructions would lead to a breach of the UK GDPR or local data protection laws.

Accountability obligations

You must comply with certain UK GDPR accountability obligations, such as maintaining records and appointing a data protection officer.

International transfers:

The UK GDPR's prohibition on transferring personal data applies equally to processors as it does to controllers. This means you must ensure that any transfer outside the UK is authorised by the controller and complies with the UK GDPR's transfer provisions.
Co-operation with supervisory authorities

You are also obliged to cooperate with supervisory authorities (such as the ICO) to help them perform their duties.

You must comply with certain UK GDPR accountability obligations, such as maintaining records and appointing a data protection officer.

Attributions

1. ICO Information Commissioner's Office

Some of the text within this document has been copied from the ICO https://ico.org.uk/

(The following items have been licensed under the Open Government License (OGL))

Name	Date Published	Document
The principles	01/01/2021	https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/
Contract	01/01/2021	https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-

		gdpr/accountability-and-governance/contracts/
What does it mean if you are a processor?	01/01/2021	https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/controllers-and-processors/what-does-it-mean-if-you-are-a-processor/#1
What does it mean if you are a controller?	01/01/2021	https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/controllers-and-processors/what-does-it-mean-if-you-are-a-controller/