



Data Protection and GDPR Policy

Version 1
Reviewed Nov 2023

The Activation Project
27 Regent Street
Leamington Spa
CV8 2TE

Introduction

The Activation Project provides strategic services to a range of clients across many different industries. We handle a range of corporate data relating to strategies, market insight and information, services and product plans, operational performance data.

In terms of data protection and GDPR, the Client Company is the controller, and The Activation Project is the processor. We do not share client confidential data with any third party organisations unless instructed to do so by a client or as part of a contractual obligation.

The data that The Activation Project processes is strictly in order to provide our services to our clients. We do not request, hold or process individual client employee or individual customer data that is deemed 'Sensitive Data' unless this is required by a contract and consented to. This means sensitive data pertaining to: gender, racial or ethnic origin; neural divergence; registered disability. However, we do not gather data related to; trade union membership; political associations or opinions; criminal offences; home addresses; the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person; or personal/financial information, client employee records including payroll information, etc.

Scope

This policy sets out The Activation Project's commitment to ensuring that any data processing is carried out in compliance with data protection law. We also strive to ensure that good data protection practice is embedded in the culture of our staff and our organisation and we follow our clients processes and procedures when processing data for them as part of our services.

This policy applies to all data processed by The Activation Project and is a part of our approach to compliance with data protection law. All The Activation Project staff are expected to comply with this policy and failure to comply may lead to disciplinary action for misconduct, including dismissal.

Its provision is also included in their employment contracts, along with confidentiality requirements.

NB: This policy is associated with our IT Security Policy for The Activation Project, and, a separate Data Protection Policy specifically for the Pulse Feedback Service.

Monitoring and review

This policy was originally created in April 2020, and shall be regularly monitored and reviewed.

Data protection principles

The Activation Project complies with the data protection principles set out below. When processing data, we ensure that:

- it is processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency')
- it is collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ('purpose limitation')
- it is all adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')
- it is all accurate and, where necessary, kept up to date and that reasonable steps will be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy')
- it is kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed ('storage limitation')
- it is processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')

and also

- it is appropriately and securely kept, which is demonstrated in our IT security Policy
- it is not transferred to any other country/third party/etc without adequate protection in situ and from The Activation Project's perspective, without the expressed knowledge or consent of the client organisation, in compliance with contractual and confidentiality agreements

The Activation Project will facilitate any request from a data subject who wishes to exercise their rights under data protection law as appropriate, always communicating in a concise, transparent, intelligible and easily accessible form and without undue delay, and where reasonable to do so.

Process/procedures/guidance

The Activation Project will:

- ensure that the legal basis for processing any data is identified in advance and that all processing complies with both the law and contractual obligations
- not do anything with any data that you would not expect given the content of this policy and the fair processing

- ensure that appropriate guidance and notices are in place advising staff and others how and why any or their data is being processed, and, in particular, advising data subjects of their rights
- only collect and process data that it needs for purposes it has identified and in connection to the service provided to our clients
- ensure that, as far as possible, the data it holds is accurate, or a system is in place for ensuring that it is kept up to date as far as possible, or with respect to strategic data, ensure that appropriate practices are in place to know when it has been superseded or out of date
- only hold onto any data for as long as it is needed, after which time or as agreed with the client in relation to client confidential data, it will be securely erased
- ensure that appropriate security measures are in place to ensure that the appropriately classified data can only be accessed by those who need to access it and that it is held and transferred securely

The Activation Project will ensure that all staff who handle personal data on its behalf are aware of their responsibilities under this policy and other relevant data protection and information security policies, and that they are adequately trained and supervised.

Data Subject Rights

We have processes in place to ensure that we can facilitate any request made by a client, a client employee or a legitimate representative acting on behalf or in association with a client, to exercise their contractual rights or under data protection law relating to their data.

All relevant staff will receive training to support this and will be able to identify such a request and know how to respond to it.

All requests will be considered without undue delay and responded to in an appropriate time frame. The maximum is 30 days unless contractually required.

Subject access: the right to request information about how client or personal data is being processed, including the right to be allowed access to what the data is and to be provided with a copy of that data along with the right to obtain the following information:

- the purpose of the processing
- to whom data has been disclosed or which will be disclosed within The Activation Project or the Client Organisation
- the agreed retention period, as defined by the data controller or by contractual obligations, where not in conflict with law

- the source of the information if not collected direct from the client or their representatives, and
- the existence of any additional decision making relating to the data or its processing

Rectification: the right to allow the client organisation or data subject to rectify inaccurate data concerning them or their specific organisation.

Erasure: the right to have data erased and to have confirmation of erasure, but only where:

- the data is no longer necessary in relation to the purpose for which it was collected, or
- where consent is withdrawn, or
- where there is no legal basis for the processing, or
- there is a contractual or legal obligation to delete data

Restriction of processing: the right to ask for certain processing to be restricted in the following circumstances:

- if the accuracy of the data is being contested, or
- if our processing is unlawful but the data subject does not want it erased, or
- if the data is no longer needed for the purpose of the processing but it is required by the data subject for another legitimate reason
- if the data subject has objected to the processing, pending verification of that objection

Data portability: the right of the client organisation to receive a copy of their data which has been provided by their employees, or the right of the data subject to receive a copy of their personal data. This would only apply if The Activation Project was processing the data using consent or on the basis of a contract.

Object to processing: the right to object to the processing of data relying on the legitimate interests processing condition unless The Activation Project can demonstrate compelling legitimate grounds for the processing which override the interests of the Client Organisation.

Restrictions on the rights of data subjects: in the event a client employee requests data that has been restricted in circulation by their client organisation, or, requests data that is not related to their client organisation and covered by separate client confidentiality, then The Activation Project retains the right to deny that request and where appropriate, communicate this request to the corresponding client organisation.

The special processing of additional personal data on behalf of a client:

In the event we are asked to, as part of a contractual obligation, process additional personal data on behalf of a client organisation, such as customer feedback data, we will strive to follow the policy and protocols of the client organisation, with the data protection principles as the guiding rule. This will be on an as-need basis.

In this instance, we will agree with the client how the data will need to be classified, processed and the safeguards which will need to be included to ensure that we comply with the data protection principles and maintain good practice.

As defined in the IT Security Policy, in the event of a breach under GDPR

Based on the ICO Self-Assessment provided by the UK Government, the data we process on behalf of our Clients does not require us to report any data breach to the information commissioner.

Therefore, in the event of a breach, our aim is:

- to secure the situation and prevent any ongoing or repeat breaches
- regain the trust of our clients in the service provided

In the event a breach happens, we follow this process, unless instructed by a client or by contractual obligations:

1) Initial investigation of the nature of the breach:

- The breach details
- Nature of the breach, including potential removal or copy of any data captured
- Risk and severity of the breach

If the breach is part of a cyber attack, we will notify Microsoft Business and the Police.

2) Notification to the Client Company(s) of the breach:

- Which includes the initial details of the breach and any initial actions required
- A timetable for full investigation

3) Full investigation of the nature of the breach

- Depending on the nature of the breach, this may include appointing an independent expert to join the investigation

4) Report on the findings

- Including the agreement with the Client Company(s) about what needs to happen
- In this step, we recommend any users whose feedback has been compromised are notified of what has happened and what is being done to correct this

- 5) Implementation of the recommendations and agreement with the Client Company(s)
 - In the time frames agreed
 - With the ability to demonstrate those actions have been taken

- 6) Post breach review
 - To determine lessons that need to be learnt, and any further actions taken

Responsibility for the processing of data

The directors of The Activation Project take ultimate responsibility for data protection.

If you have any concerns or wish to exercise any of your rights under the GDPR, then you can contact them via support@activationproject.org

Definitions:

Client Company/Client Organisation: The client organisation – the controller - that owns the data and requests our services as part of a contract relationship, with a requirement to process data on their behalf.

Data Processor: The Activation Project processes data as collected and provided by Client Organisations. The Client Organisation will always be and retain the ownership of the original and processed data.

Data Subject: a client sponsor, client lead contact, a client employee or a legitimate representative acting on behalf or in association with a client, and to whom the data may relate. This may include both client organisation data such as strategies, market insight and information, services and product plans, operational performance data, as well as personal data such as received emails together with associated business email address and business contact details.