

Data Protection Policy - GDPR

1 Introduction

This policy refers to the General Data Protection Regulation (EU) 2016/679 (GDPR). GDPR applies to 'personal data', that is any data that can directly or indirectly identify an individual. This includes, name, address, telephone number, email and identifier codes. It also refers to 'sensitive personal data' as stated in Article 9.

Keyturn Training Limited needs to keep certain information about its employees, customers and suppliers for financial and commercial reasons and to enable us to monitor performance, to ensure legal compliance and for health and safety purposes. To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. Keyturn Training Limited complies with the Data Protection Principles set out in the General Data Protection Regulation.

2 Security policy and responsibilities in the company

- Personal data shall be processed fairly and lawfully and in a transparent manner in relation to individuals.
- All data is collected for a specified, explicit and legitimate purpose as agreed with the individual
- The use of data is adequate, relevant and limited to what is necessary in relation to the purpose for which they are being processed
- Kept in a form that allows Keyturn to remove data when no longer necessary or requested to be moved
- Data is processed securely to prevent accidental loss or damage
- There is a commitment to continuous improvement of data management
- Awareness and training for all employees and contracted staff is essential

3 1.3 The lawful basis for processing data – reference GDPR article 6 (1) and Article 6 (2) and Recital 40

There are six given reasons for why an organisation would have personal data. The data that Keyturn obtain and use is based on these lawful reasons:

- Consent – individuals have given clear instruction for Keyturn to hold their data for a specific purpose. Where consent is given Keyturn will make sure that the individual is aware of:
 - who Keyturn is
 - any third party that will have access to the data (if applicable)
 - why Keyturn want the data
 - what Keyturn will do with the data
 - how they can withdraw their consent at any time
- Contract – the processing of an individual's data is necessary to fulfil the contract the individual has signed.

- The verbal contract starts when an individual requests information on our service for a specific reason
- The written contract starts when the individual has agreed on the service and signed an order
- On both accounts Keyturn will inform the individual of what data is being held as per point 5.2
- Legal Obligation – where it is necessary to process data from a legal requirement
 - The legal obligations are based on UK or EU law
 - Where legal reasons apply data will be passed on to third parties (e.g. HMRC with employee salary details)
- Vital Interests – where the processing of data is necessary to protect someone’s life
 - Where Keyturn deem it important to hold data for vital interest, the data will be held securely with limited access to personnel
 - Explicit consent will be requested in collecting this data
- Public task – using the data to perform a task in the public interest or official functions
 - This includes carrying out a specific task in the public interest which is laid down by law; or
 - exercising official authority which is laid down by law (domestic or EU law)
 - where this basis applies Keyturn will inform individuals to gain consent
- Legitimate interests – where there is a legitimate interest in the information Keyturn provide, or service offered
 - Keyturn use data under the legitimate interest’s basis making sure that it is what the individual would expect and that it has a minimal privacy impact
 - Keyturn’s policy outlines in section 5 the legitimate interest, the data held and why it is being processed
 - Article 6(1)(f) states that “processing is necessary for the purposes of the legitimate interests pursued by the controller (Keyturn) or by a third party except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.”
 - When using legitimate interests for direct marketing, the right to object is absolute and Keyturn will stop processing the data immediately

4 Individuals rights

As part of the GDPR Keyturn follow the guidelines for the rights for individuals, as stated in GDPR these are:

- The right to be informed – Keyturn inform all individuals with privacy information which allows the individual to see what data we hold on to, the purpose of processing it, the lawful basis for processing the data. Clear guidance is given to the individual along with details of Keyturn and primary contacts for any data concerns
- The right of access – individuals have the right to access their personal data and supplementary information. Keyturn will comply with the request within one month, where data is more complex it may be extended by a further two months
- The right to rectification – individuals can request that personal data is corrected or complete any incomplete data. Keyturn will rectify the information within one month of request
- The right to erasure – where an individual requests the right to erasure for personal data that is no longer necessary or is prior to contract (i.e. used primarily for marketing purposes) Keyturn will comply immediately. This may include Keyturn contacting any third parties that may also have access to the data

- The right to restrict processing – Keyturn will make any restricted data unavailable to users upon request. Where data is required for safety or legal reasons, Keyturn will discuss with the individual. Keyturn will act on this request immediately
- The right to data portability – individuals can move, copy or transfer personal data for their own use. Keyturn will respond to this request within one month
- The right to object – where an individual's data is kept on the basis of legitimate interest, such as marketing, they have the right to object. Where Keyturn can demonstrate compelling legitimate grounds for the processing or if the processing has a legal requirement, the individual will be informed and agreement will be put in to place. Individuals have the right to object at the point of first contact and is mentioned in Keyturn's privacy policy
- Rights in relation to automated decision making and profiling – Keyturn's processing does not match this definition, however if that should change information on profiling will be found on the privacy policy

5 Documentation

Under Article 30(1) of the GDPR the personal data we process is as follows:

5.1 Data used for Marketing Purposes – Potential Customers/Clients

- Data used for sales and marketing purposes are opt in data
- The data is a mixture of opt in and legitimate interests, Keyturn process data of organisations and relevant contacts with in that organisation that have a role relevant to the service Keyturn provide
- If at any point an individual or organisation wish to have their data removed or unsubscribe from emails or telephone calls, this will be done immediately upon request
- This data is reviewed on an annual basis and where it falls outside of legitimate interest it will be removed
- Where individuals are receiving emails, Keyturn will email on an annual basis to opt in to continue to receive marketing emails
- Data that is held for marketing purposes includes, organisation name, telephone, address, individual responsible for managing the training needs, job title and email address
- All data is held on a secure database that is accessed by authorised personnel within Keyturn as directed by the board

5.2 Data used for Sales Purposes – Customers/Clients

As per 'data used for marketing purposes' in addition:

- As soon as an order/contract is signed there is additional data that will be required to deliver the service required
- The data used following an order/contract includes primary contact name, job title, telephone and email. Admin contact name, job title, telephone and email. This data is used to make sure that all projects and services being delivered function to the benefit of the client
- This data is only used for marketing if the individual has requested it
- This data is kept on a database that is only accessed by the relevant personnel. Once an order is signed the data passes through to the projects and finance department

- Notes of relevance conversations are also kept on the database, this data is reviewed on an annual basis to make sure it is still relevant to the service we are providing to Keyturn customers

5.3 Data used for Project Purposes – Customers/Clients

- As soon as a client signs a sales contract/order the data passed to our projects team includes primary contact name, job title, telephone and email. Admin contact name, job title, telephone and email
- Keyturn provide training for organisations throughout the UK, this requires regular contact with organisations to make sure that all information we have is correct. This data is kept for 2 years to enable us to monitor performance, with individuals within the organisation receiving the service
- For each project Keyturn run, data that is collected from organisations is only used to inform, assess and review the development of those individuals which can be directly or via a nominated contact within the organisation
- This data is kept secure to eliminate any loss or damage
- Data used for the projects include individual names, organisation name and telephone numbers. In some cases where requested by the client email addresses and job titles will also be obtained
- This data is used by our staff and contracted training delivery team. Our contracted staff have signed a contract to agree to the above terms of data.
- Keyturn contracted staff will not keep any data beyond a week following the workshop unless special requests have been made by the individuals
- All data given to the contracted staff will be returned to Keyturn via special mail or scanned and emailed, any additional data not required by Keyturn or the client will be removed
- Each learner will be sent a link to our data protection policy within the joining instructions which are sent prior to the learning event
- Customers will be informed of our data protection policy within the contract they sign at the beginning of the working relationship

5.4 Data used for Finance Purposes – Customers/Clients/Suppliers

- All data is kept in a centralised secure location that is only accessed by the Keyturn finance team
- Data is collected from sales orders/contracts and is held by the finance team in order to produce invoices
- Data from supplier invoices are held in order to pay suppliers
- Data from both the sales orders/contracts and supplier invoices are kept for seven years as per the requirement of our accountants
- This data is not used for marketing purposes, but solely for financial purposes which includes, generating invoices, requested purchase order numbers, chasing payment, making payment, and any other additional financial requirement
- Keyturn accountants have access to our financial information and they have provided Keyturn with their GDPR policy

5.5 Data used for Personnel Purposes – Internal Staff/Contractors

- Data of employees is kept in a secure location and is only accessible by the directors
- This data kept on employees is name, address, telephone number, emergency contact details, appraisal documentation, disciplinary notes, holiday forms, sickness forms, salary and pension information, contracts
- All data kept on employees is used for either health and safety, emergency, managing performance, maintaining monthly salary payments, calculating annual holidays, calculating statutory pension payments as per the terms and conditions of employment
- Employee data is kept during the employment plus an additional six years after they have left. This is due to legal obligations
- Employees have the right to erasure following employment but not during employment
- CV's are kept on file for a minimum of six months, and reviewed depending on requirement (i.e. a potential trainer's CV will be kept longer for the purposes of responding to internal and external quality assessment for Keyturn's qualification programmes)

5.6 Data used for Qualifications – Learners

In addition to the above, those clients that choose to go the qualifications route, additional data will be required. This includes learners name, date of birth, nationality and contact details. This data is used for both ILM qualifications and Apprenticeships. This data is then inputted on to the ILM database to set up their membership and qualification status. More information on how to access the ILM personal data policy for learners can be found here - <https://www.i-l-m.com/privacy/learnerspersonaldata>

6 Data security

Appropriate technical and organisational measures are implemented to make sure data is kept safe. With the relevant software, reviews and updates put in place.

Administrative and managerial processes and procedures are put in place to make sure that data is used correctly, legally and securely. This is reviewed on a regular basis by the board of directors. The Data Protection Officer is on the board of directors.

For more information or if you have any questions regarding your use of data please do not hesitate to contact us on enq@keyturn.co.uk

Further information can be accessed on additional privacy and data protection policies:

[Website Privacy Policy](#) (Keyturn documentation)

[Privacy Policy](#) (Keyturn documentation)

[Training Team and Contracted Staff Policy](#) (Keyturn documentation)

[ILM Learner Personal Data \(ILM Qualifications\)](#)

[Microsoft Dynamics Data](#) (Keyturn's data system)

[Inscape Epic Privacy Data](#) (when completing online behaviour profiles)

Updates/Reviews		
14 April 2018	Full creation	CJS