Data Protection Policy – General Data Protection Regulation 2018 (GDPR)

This document can be made available in other formats- on request.

Version 1.1
Published: 25th May 2018
Drafted by: Connor McDonald
Approved by: Mark Tickle/ Ian Pilkington

Rationale:

First Logistics is committed to a policy of protecting the rights and privacy of individuals, including our temporary workers, office staff, customers and others, in accordance with the General Data Protection Regulation (GDPR) May 2018.

The new regulatory environment demands higher transparency and accountability in how we manage and use personal data. It also accords new and stronger rights for individuals to understand and control that use.

The GDPR contains provisions that First Logistics will need to be aware of as data controllers. For example, the GDPR requires that:

We must ensure that our privacy notices are written in a clear, plain way that our staff, workers and customers will understand.

First Logistics needs to process certain information about its staff, temporary workers, contractors, sub-contractors, job seekers (e.g. applicants for temporary and permanent work we have advertised) customers and other individuals with whom we have relationships with for various purposes such as, but not limited to:

1. The recruitment and payment of staff, contractors, sub-contractors, temporary workers.
2. The payment to customers.
3. The general day to day administration purposes of the business.
4. Complying with statutory obligations to government bodies, insurers and local government.
5. Receiving payment from customers and keeping accurate records of payments.
6. Maintaining accurate records that our insurers, or our customer's insurers may require.

To comply with various legal obligations, including the obligations imposed on it by the General Data Protection Regulation (GDPR) First Logistics must ensure that all this information about individuals is collected and used fairly, stored safely and securely, and not disclosed to any third party unlawfully.

Compliance:

This policy applies to all staff of First Logistics. Any breach of this policy or of the Regulation itself will be considered an offence and disciplinary procedures will be invoked.

As a matter of best practice, other external agencies and individuals working with First Logistics who have access to personal information, will be expected to read and comply with this policy. It is highly unlikely that this will ever happen.

This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments to the GDPR and other relevant legislation.

General Data Protection Regulation (GDPR):

This piece of legislation comes into force on the 25th May 2018. The GDPR regulates the processing of personal data, and protects the rights and privacy of all living individuals. For example, by giving all individuals who are the subject of personal data a general right of access to the personal data which relates to them. Individuals can exercise the right to gain access to their information by means of a 'subject access request'. Personal data is information relating to an individual and may be in hard or soft copy (paper/manual files; electronic records; photographs; CCTV images) and may include facts or opinions about a person.

Responsibilities under the GDPR:

First Logistics will be the 'data controller' and 'data processer' under the terms of the legislation – this means it is ultimately responsible for controlling the use and processing of the personal data. First Logistics appoints a Data Protection Officer (DPO), currently the person who is appointed as Data Protection Officer is Mark Tickle, Operations Director. Mark is the main point of contact for addressing any concerns regarding the data held by First Logistics and how it is processed, held and used.

The Driving Consultants, Jason Lonsdale and Connor McDonald are responsible for all day-to day data protection matters, and will be responsible for ensuring compliance with GDPR in relation to the day to day running of First Logistics.

Mark Tickle is also responsible for ensuring that First Logistics notification is kept accurate. Detail of First Logistics notification can be found on the Office of the Information Commissioner's website. Our data registration number is: ZA291544.

Individuals who provide personal data to First Logistics are responsible for ensuring that the information is accurate and up-to-date.

Data Protection Principles:

The legislation places a responsibility on every data controller and data processer to process and control personal data in accordance with the eight principles. More detailed and in depth guidance on how to comply with these principles can be found in the DPCop. Please follow this link to the ICO's website (www.ico.gov.uk).

In order to comply with its obligations, First Logistics undertakes to adhere to the twelve principles as outlined by the ICO:

1. Process personal data fairly and lawfully.

First Logistics will make all reasonable efforts to ensure that individuals who are the focus of the personal data (data subjects) are informed of the identity of the data controller, the purposes of the processing, any disclosures to third parties that are envisaged; given an indication of the period for which the data will be kept, any other information which may be relevant.

2. Process data for the specific and lawful purpose for which it collected that data and not further process the data in a manner incompatible with this purpose.

First Logistics will ensure that the reason for which it collected the data originally is the only reason for which it processes those data, unless the individual is informed of any additional processing before it takes place.

3. Ensure that the data is adequate, relevant and not excessive in relation to the purpose for which it is processed.

First Logistics will not seek to collect any personal data which is not strictly necessary for the purpose for which it was obtained. Forms for collecting data will always be drafted with this in mind. If any irrelevant data are given by individuals, they will be destroyed immediately.

4. Keep personal data accurate and, where necessary, up to date.

First Logistics will review and update all data on a regular basis. It is the responsibility of the individuals giving their personal data to ensure that this is accurate, and each individual should notify First Logistics if, for example, a change in circumstances mean that the data needs to be updated. It is the responsibility of First Logistics to ensure that any notification regarding he change is noted and acted on.

5. Only keep personal data for as long as necessary.

First Logistics undertakes not to retain personal data for any longer than is necessary to ensure compliance with the legislation, and any other statutory requirements. This means First Logistics will undertake a regular review of the information held and implement a weeding process.

First Logistics will dispose of any personal data in a way that protects the rights and privacy of the individual concerned (e.g. secure electronic deletion, shredding and disposal of hard copy files as confidential waste) A log will be kept of the records destroyed.

6. Process personal data in accordance with the rights of the data subject under the legislation.

Individuals have various rights under the legislation including a right to:

- Be told the nature of the information First Logistics holds and any parties to whom this may be disclosed.
- Prevent processing likely to cause damage or distress.
- Prevent processing for purposes of direct marketing
- Be informed about the mechanics of any automated decision making process that will significantly affect them.
- Not have significant decisions that will affect them taken solely by automated process.
- Take action to rectify, block, erase or destroy inaccurate data.
- Request that the Office of the Information Commissioner assess whether any provision of the Act has been contravened.

First Logistics will only process personal data in accordance with individuals' rights.

7. Put appropriate technical and organisational measures in place against unauthorised or unlawful processing of personal data, and against accidental loss or destruction of data.

All members of staff are responsible for ensuring that any personal data which they hold is kept securely and not disclosed to any unauthorised third parties.

First Logistics will ensure that all personal data is accessible to only those who have a valid reason for using it.

First Logistics has in place appropriate security measures e.g.
Ensuring that hard copy personal data is kept in lockable filing cabinets/ cupboards with controlled access (with the keys then held securely in a key cabinet with controlled access):

- Keeping all personal data in a lockable cabinet with key-controlled access.
- Password protecting personal data held electronically.
- Archiving personal data which are then kept securely in a lockable unit.
- Ensuring that PC Screens are not left unattended without a password protected screen-saver being used.

In addition, First Logistics enforces appropriate measures for the deletion of personal data – manual records will be shredded or disposed of as 'confidential waste' and appropriate contract terms will be put in place with any third parties undertaking this work. Hard drives of redundant PCs will be wiped clean before disposal or if that is not possible, destroyed physically. A log will be kept of the records destroyed.

This policy also applies to staff and students who process personal data 'off-site', e.g. when working at home, and in circumstances additional care must be taken regarding the security of the data.

8. Ensure that no personal data is transferred to a country or a territory outside the European Economic Area (EEA) unless that country or territory ensures adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

First Logistics will not transfer data to such territories without the explicit consent of the individual. This also applies to publishing information on the Internet- because transfer of data can include placing data on a website that can be accessed from outside the EEA.

First Logistics will always seek consent of individuals before placing any personal data (including photographs) on its website, or in the instances of sending our customer's details to customers for the purpose of obtaining a candidate/individual full time permanent work.

9. Processing of Children's Personal Data:

First Logistics does not process children's personal data. Due to the nature of our business, This element will not change.

10. Right of data portability:

The ICO defines Data Portability as: having processes to allow individuals to move, copy or transfer their personal data from one IT environment to another in a safe and secure way, without hindrance to usability.
It is highly unlikely that individuals would wish to transfer their personal data gathered for the purposes of employment/ engagement from one IT environment into another. Our business will, should that need arise facilitate this, in accordance with the requirements of GDPR.

11.Consent as a basis for processing:

Although it is not always necessary to gain consent from individuals before processing their data, it is often the best way to ensure that data is collected and processed in an open and transparent manner.

Consent is especially important when First Logistics is processing any sensitive data, as defined by the legislation.

First Logistics understands consent to mean that the individual has been fully informed of the intended processing and has signified their agreement (e.g. via the registration pack) whilst being of a sound mind and without having any undue influence exerted upon them. Consent obtained on the basis of misleading information will not be a valid basis for fair processing. Consent cannot be inferred from the non-response to a communication.

“Personal Details”

- For the purposes of the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679 you consent to First Logistics holding and processing personal data including sensitive personal data of which you are the subject, details of which are specified in the above subtext.
- This will include CCTV Imagery and recordings onsite.

First Logistics will ensure that any forms used to gather data on an individual will contain a statement (fair data collection and processing notice) explaining the use of that data, how the data may be disclosed and also indicate whether or not the individual needs to consent to the processing.

First Logistics will ensure that if the individual does not give their consent for the processing, and there is no other lawful basis on which to process the data, then steps will be taken to ensure that processing of that data does not take place.

12. Subject Access Rights (SARs):

Individuals have a right to access any personal data relating to them which are held by First Logistics. Any individual wishing to exercise this right should apply in writing to The Data Protection Officer. Any member of staff receiving a SAR should forward this to the Data Protection Officer.

First Logistics reserves the right to charge a fee for data subject access requests. (Currently £50.00

Under the terms of the legislation, any such requests must be complied with within thirty days.

Where the Data Protection Officer /First Logistics deems a SAR to be unreasonable or not based on proper grounds we will respond in writing within thirty days and will outline why the decision was made.

Disclosure of Data:

First Logistics undertakes not to disclose personal data to unauthorised third parties, including family members, friends and in some circumstances, the police.

Legitimate disclosures may occur in the following instances:

- The Individual has given their consent to the disclosure.
- The disclosure is required for the performance of a contract
- A statutory body requires the data, in this case all data will be disclosed in accordance with the Data Protection Act 2018 (as amended) and the General Data Protection Act 2018.

For detailed guidance on disclosures please consult the ICO's Code of Practice on www.ico.gov.uk.

In no circumstances will First Logistics sell any of its databases to a third party.
It is also First Logistics' policy not to purchase databases or any other form of personal data.

Email:

It is the policy of First Logistics to ensure that senders and recipients of email are made aware that under the DPA, and Freedom of Information Legislation, the contents of email may have to be disclosed in response to a request for information. One means by which this will be communicated will be by a disclaimer on all email correspondence from First Logistics staff members.

Under the Regulation of Investigatory Powers Act 2000, Lawful Business Practice Regulations, any email sent to or from First Logistics Limited. May be accessed by someone other than the recipient for system management and security purposes.

CCTV:

There are some CCTV systems operating within First Logistics for the purpose of protecting staff and property. First Logistics will only process personal data obtained by the CCTV system in a manner which ensures compliance with the legislation.

First Logistics, may at some stage in the future utilise Automatic Number Plate Recognition (ANPR) to ensure the safety and security of its onsite staff.

Data chain of custody:

First Logistics collect personal data on individuals in order for us to find work and place temporary staff with our clients.

The information our candidates / temporary and contract workers and employees provide to us is controlled and processed for the following reasons:

- To assess suitability for placement with our clients – e.g. by obtaining details of qualifications and previous experience and employment details so that we can accurately place our candidates.
- References/ details of recommendations will be kept in paper copy to verify suitability for engagement/ employment.
- To ensure compliance with our and our client's insurance criteria.
- To ensure we are protecting the Health and Safety of our temporary workers, contractors and office staff by obtaining previous details of previous health conditions, pre-existing health conditions and by obtaining details of previous medication taken.
- Bank/building society details, National Insurance number, P45/Starter Checklist (P46) forms. This data is retained to ensure compliance with Statutory PAYE reporting requirements and to ensure accurate payment to our temporary workers, contractors and office staff.
- For Limited Company contractors we obtain details of their business bank account, company registration number, company name, VAT Registration number (if applicable), UTR number (if applicable), business banking details, and details of public liability insurance. Again, this data is retained to ensure compliance with statutory reporting obligations we have to HMRC.
- Details of previous criminal convictions will be obtained and recorded in accordance with the Rehabilitation of Offenders Act 1974. Extensive data which outlines offences, convictions and the outcome of such offences will be kept in paper and electronically. We have a 'Fair Data Processing Notice' which is contained in our registration packs which informs potential contractors/candidates/temporary workers/ employees that by providing details of previous convictions/ offences – which we may have to disclose this information to our customers for compliance purposes. All disclosures in relation to the Rehabilitation of Offenders Act 1974 will be done with the upmost professionalism and in accordance with the Data Protection Act 2018, General Data Protection Regulation 2018, and The Rehabilitation of Offenders Act 1984.

The Data Protection Officer, Mark Tickle, alongside Ian Pilkington, Jason Lonsdale and Connor McDonald have responsibility for ensuring that the personal data provided is handled and respected in accordance with this policy.

Flow of personal data within First Logistics:

Concerning the engagement of PAYE Temporary Workers, Contractors and Limited Company temporary workers.

1. Registration Process:

Potential candidates are invited to register at our offices in Bury.

Registration form QOF(R) is completed by the candidate.

Copies of the candidate's qualifications, references, previous employment history, medical history, payment details , right to work documentation and insurance details (if applicable) are obtained

2. Input onto VDQ:

After acceptance for an assignment, the candidate's data from Registration form QOF(R) is then entered onto our secure cloud based Operating System VDQ.

This data is kept on VDQ in line with statutory requirements, and is fully deleted after this data is no longer required.

3. Input onto Payroll System:

The candidate's payroll information contained in QOF(R) is then entered onto our secure payroll system, so that our temporary workers, contractors and employees can be paid accurately.

4. Securely filed:

The candidate's registration form QOF(R), is then securely stowed away in our secure filing cabinet. Access to this cabinet is restricted to authorised personell only and the key is securely held. If the candidate ceases to work for us, we securely archive their registration form (QOF (R) in our secure archiving unit. Access to the archives is restricted to the company directors only.

5. Data Management and Secure Disposal:

We at First Logistics take our responsibilites of managing personal data very seriously. Any data provided that isn't deemed necessary to be held is securely disposed of in accordance with the Data Protection Act 1998 and the General Data Protection Regulations 2018. Any data held electronically is securely deleted from VDQ and any data contained as a 'paper copy' is securely disposed of using our secure shredding contractor. A log of all data disposed of is retained.

Retention of personal data:

Owing to certain statutory requirements from bodies such as, but not limited to: Her Majesty's Revenue and Customs (HMRC), Department for Work and Pensions (DWP), Local Authorities, Governmental bodies and departments, and certain emergency services such as the Police. We must keep certain types of data so that they are available for inspection.

Personal Data Retention Guidelines:

Type of Data	***Retained for***
Candidate Registration data from Registration Pack QOF(R), both contained in VDQ and on Paper	***Six years*** - Data on VDQ is deleted and Paper copies are securely disposed of via our secure external contractor.
Candidate/ Contractor/ Employee timesheets	***Two years –*** Electronic copies are securely deleted, and paper copies are disposed of via our secure external contractor.
Invoices from contractors and their insurance details	***Seven years –*** Electronic copies are securely deleted, and paper copies are disposed of via our secure external contractor.
Payroll Information, correspondence from HMRC, Pension Bodies, the courts, or other bodies that may require us to make statutory deductions from a person(s) wages.	***Seven years –*** Electronic copies are securely deleted, and paper copies are disposed of via our secure external contractor.
Any miscellaneous correspondence or other data collected in accordance with the Data Protection Act 2018 & General Data Protection Regulation 2018.	The data collected will be disposed of in accordance to statutory requirements and will be disposed of in accordance with the Data Protection Act 2018 & General Data Protection Regulation 2018. The directors, may at their discretion, securely dispose of or securely retain such data where there is no statutory requirement imposed on timescales for disposal.
CCTV Recordings and pictures obtained on site.	Such data will be held in accordance with the Data Protection Act 2018 and General Data Protection Regulation 2018.First Logistics abide by the Information Commissioner's Office's (ICO) Code of Practice for the operation of CCTV and the subsequent storage of the data.

Data Protection Impact Assessments (DPIA):

Under the GDPR, larger organisations may need to conduct a DPIA, the below is excerpt is taken from the Information Commissioner's Office (ICO).

Below is our explanation in red, as to why it is not necessary for First Logistics to undertake a DPIA.

"You must carry out a DPIA when:

* Using new technologies; and *this is not applicable to First Logistics, we have two systems that store/process data that have been in use for a number of years – this is highly unlikely to ever change.*

* When the processing is likely to result in a high risk to the rights and freedoms of individuals. *We only process data from the registration form and wages.*

Processing that is likely to result in a high risk includes but is not limited to:

* Systematic and extensive processing activities, including profiling and where decisions that have legal effects – or similarly significant effects – on individuals; *This is not applicable to the activities of First Logistics.*

* Large scale processing of special categories of data or personal data relation to criminal convictions or offences; and *This is not applicable to the activities of First Logistics.*

* Large scale systematic monitoring of public areas. *We have two CCTV cameras which cover the main car park.*

First Logistics therefore deems undertaking a DPIA as unnecessary.

Responding to Data Breaches & Our Security Policy

First Logistics has a system in place which enables us to identify potential data breaches and how to respond to them, please see below:

Detection of a Data Breach:

- If this is an 'electronic' breach our third party IT company and VDQ, our cloud based system will alert us immediately to any breaches, attempted breach through or unauthorised access.
- The DPO Mark Tickle, will then immediately report this breach or suspected breach to the ICO and will advise Connor McDonald and Jason Lonsdale of further action to take.
- As our IT systems are cloud based and remotely operated, we can immediately facilitate a full shut down to secure our data.
- The DPO will then log and record details of the breach / suspected breach, including details of those whose data is affected.
- If this is a 'hard' breach e.g. theft of our IT system, theft of paper records the incident will be immediately reported to the Police.
- The DPO Mark Tickle, will then immediately report this breach or suspected breach to the ICO and will advise Connor McDonald and Jason Lonsdale of further action to take.

- In both instances of breach or suspected breach, which is likely to result in a high risk of adversely affecting individual's rights and freedoms, we will immediately inform those individuals without undue delay.

Security Policy:

First Logistics are fortunate enough to operate a secure, cloud based data storage system (VDQ and Payroll). Two-step log in authentication is required in order to access this information. Remote access is not available as well, so data can only be accessed in the office.

The four current authorised users for VDQ are:

Mark Tickle – Operations Director
Ian Pilkington – Finance Director
Connor McDonald – Senior Driving Consultant
Jason Lonsdale – Driving Consultant.

The three current authorised users for Payroll are:

Mark Tickle- Operations Director
Ian Pilkington – Finance Director
Connor McDonald – Senior Driving Consultant

Where a user ceases to be in employment with First Logistics, their access rights to these systems will be immediately revoked.

In order to maintain the highest levels of I.T. & Paper record security & integrity, First Logistics staff will always:

- Log off their computers prior to going home to ensure there cannot be any unauthorised.
- Routinely change their passwords to ensure the threat of unauthorised access is minimised.
- Where possible send documentation in a PDF format to reduce the risk of unauthorised editing.
- If an email is mistakenly sent to an unwanted recipient immediately inform them and seek to recover the email immediately.
- Routinely delete data from their email if not required any longer.
- Update their Anti-Virus software when recommended to ensure the highest levels of protection are maintained.
- Update their operating software when recommended to ensure the highest levels of protection are maintained.
- Report any attempts of unauthorised access to the Directors immediately.
- Contact VDQ or Payroll if they detect any issues with the cloud based software.
- Lock paper records away securely and lock their drawers prior to going home.
- Correctly dispose of paper data in the designated paper disposal bags when the paper data is no longer required.
- Report any concerns or suspicious activity immediately to the Directors.
- Only give the 'On-Call' mobile phone to authorised members of staff, this mobile is password protected and securely tracked.

Action Points:

In order to respond effectively to the new GDPR, First Logistics has undertaken the following:

- Drafted a Data Protection Policy, available for viewing in multiple formats.
- Provided our internal office staff with a copy of this policy so that our driving consultants are aware of their increased responsibilities to protect data under the GDPR.
- Will ensure that any new starters in the office are aware of their responsibilities under GDPR by providing them with a copy of this policy.
- Re-written our Privacy Policy and placed an updated version of this on our website
- Placed a copy of our Data Protection Policy on our website.
- Communicated to our existing staff informing them of their increased rights under the GDPR, e.g. SAR and asked for a response slip confirming they provide consent for us to hold their data in accordance with the GDPR.
- Updated our e-mail disclaimers to ensure they are up-to-date with GDPR
- Revised our registration documentation for candidates, so that they are fully aware of why we require their data, how it is processed, controlled and stored, their SAR's, along with obtaining positive consent with an 'opt-in' box at the end of this disclaimer.

Contact Details:

First Logistics:

Mark Tickle (DPO)
First Logistics
Unit 4 The Old Courthouse
Tenterden Street
Bury
BL9 0AL

T: (0161) 832 4111
E: info@firstlogistics.co.uk
W: www.firstlogistics.co.uk

Information Commissioners Office (ICO)

T: (0303) 123 1113
E: casework@ico.org.uk
W: https://ico.org.uk

Useful documents which are held on file and are available upon request:

CCTV Code of Practice (Published by the ICO).
Guide to the General Data Protection Regulation (Published by the ICO).
Guide to PECR (Published by the ICO).
First Logistics ICO registration.

THIS PAGE IS LEFT INTENTIONALLY BLANK.