



# General Data Protection Policy

| Document Information     |                                                                                                                                              |
|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Document Name:</b>    | General Data Protection Policy                                                                                                               |
| <b>Author's Name:</b>    | Morgan Bailas                                                                                                                                |
| <b>Date of Creation:</b> | 01/05/2018                                                                                                                                   |
| Document Distribution    |                                                                                                                                              |
| IT, DPO                  |                                                                                                                                              |
| Document Change Control  |                                                                                                                                              |
| Change Reference         | Detail of Change                                                                                                                             |
| <b>Version 2.0</b>       | Document review – 01/10/21 – Ian Dawson                                                                                                      |
| <b>Version 2.1</b>       | Updated look and FRA logo, Review – 05/01/23 – Kieran Barker                                                                                 |
| <b>Version 2.2</b>       | 11-March-2023 Updated DPO from Ian Dawson to Morgan Bailas.                                                                                  |
| <b>Version 3.0</b>       | Document review, large scale EFI Group updates, Staff Training (19) and CCTV (19) section amendments - Chris Maja and Morgan Bailas 14/03/24 |
| <b>Version 3.1</b>       | Update to Transparent Processing (7.1), CCTV (18) Document review - Morgan Bailas 20/03/25                                                   |

**TABLE OF CONTENTS**

- 1. OVERVIEW ..... 3
- 2. ABOUT THIS POLICY ..... 3
- 3. DEFINITIONS ..... 3
- 4. EFI GROUP PERSONNEL’S GENERAL OBLIGATIONS ..... 5
- 5. DATA PROTECTION PRINCIPLES ..... 5
- 6. LAWFUL USE OF PERSONAL DATA ..... 6
- 7. TRANSPARENT PROCESSING – PRIVACY NOTICES ..... 7
- 8. DATA QUALITY – ENSURING THE USE OF ACCURATE, UP TO DATE AND ..... 7  
RELEVANT PERSONAL DATA ..... 7
- 9. PERSONAL DATA MUST NOT BE KEPT FOR LONGER THAN NEEDED ..... 8
- 10. DATA SECURITY ..... 9
- 11. DATA BREACH ..... 9
- 12. APPOINTING CONTRACTORS WHO ACCESS THE EFI GROUP OR SUBSIDIARY  
COMPANY PERSONAL DATA ..... 10
- 13. INDIVIDUALS’ RIGHTS ..... 11
- 14. MARKETING AND CONSENT ..... 12
- 15. AUTOMATED DECISION MAKING AND PROFILING ..... 13
- 16. DATA PROTECTION IMPACT ASSESSMENTS (DPIA) ..... 14
- 17. TRANSFERRING PERSONAL DATA TO A COUNTRY OUTSIDE THE EEA ..... 15
- 18. CCTV ..... 15
- 19. Training ..... 15

## 1. OVERVIEW

The EFI Group's reputation and future growth are dependent on the way the EFI Group and subsidiary companies manage and protect Personal Data. Protecting the confidentiality and integrity of Personal Data is a key responsibility of everyone within the EFI Group and all subsidiary companies.

As an organisation the EFI Group and its subsidiary companies collect, use, and store Personal Data about its employees, suppliers, academic partnerships or individuals within companies, students, governors, parents, and visitors. The EFI Group recognises that having controls around the collection, use, retention and destruction of Personal Data is important in order to comply with their obligations under Data Protection Laws and in particular its obligations under Article 5 of GDPR.

The EFI Group has implemented this Data Protection Policy to ensure all EFI Group and subsidiary company Personnel are aware of what they must do to ensure the correct and lawful treatment of Personal Data.

EFI Group and subsidiary company Personnel will receive a copy of this Policy when they start and may receive periodic revisions of this Policy. This Policy does not form part of any contract of employment and the EFI Group reserves the right to change this Policy at any time. All members of EFI Group and subsidiary company Personnel are obliged to comply with this Policy at all times.

If you have any queries concerning this Policy, please contact our Data Protection Officer, who is responsible for ensuring the EFI Group and subsidiary company's compliance with this Policy.

## 2. ABOUT THIS POLICY

This Policy (and the other policies and documents referred to in it) sets out the basis on which the EFI Group and subsidiary companies will collect and use Personal Data either where the organisation collects it from individuals itself, or where it is provided to the organisation by third parties. It also sets out rules on how the EFI Group and subsidiary companies use, transfer and store Personal Data.

It applies to all Personal Data stored electronically, in paper form, or otherwise.

## 3. DEFINITIONS

**3.1. Fashion Retail Academy** – The Fashion Retail Academy (a trading name of EFI Group)

**3.2. EFI Group Personnel** – Any EFI Group employee, worker or contractor who accesses any of the Fashion Retail Academy's Personal Data and will include employees, consultants, contractors, and temporary Personnel hired to work on behalf of the Fashion Retail Academy.

**3.3 Subsidiary Company** – Any company owned, or part-owned by EFI Group.

**3.4. Controller** – Any entity (e.g. company, organisation or person) that makes its own decisions about how it is going to collect and use Personal Data.

A Controller is responsible for compliance with Data Protection Laws. Examples of Personal Data that the EFI Group are the Controller for includes employee details or information the EFI Group collects relating to students. The EFI Group will be viewed as a Controller of Personal Data if it decides what Personal Data the EFI Group is going to collect and how it will use it.

A common misconception is that individuals within organisations are the Controllers. This is not the case it is the organisation itself which is the Controller.

**3.5. Data Protection Laws** – The General Data Protection Regulation all applicable laws relating to the collection and use of Personal Data and privacy and any applicable codes of practice issued by a regulator including in the UK, the Data Protection Act 2018.

**3.6. Data Protection Officer** – The EFI Group Data Protection Officer is Morgan Bailas, and can be contacted at: 02073072365 [DPO@fra.ac.uk](mailto:DPO@fra.ac.uk)

**3.7. EEA** – Austria, Belgium, Bulgaria, Croatia, Republic of Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden.

**3.8. ICO** – the Information Commissioner’s Office, the UK’s data protection regulator.

**3.9. Individuals** – Living individuals who can be identified, *directly or indirectly*, from information that the EFI Group or subsidiary company have. For example, an individual could be identified directly by name, or indirectly by gender, job role and office location if you can use this information to work out who they are. Individuals include employees, students, parents, visitors and potential students. Individuals also include partnerships and sole traders.

**3.10. Personal Data** – Any information about an Individual (see definition above) which identifies them or allows them to be identified in conjunction with other information that is held. It includes information of this type, even if used in a business context.

Personal data is defined broadly and covers things such as name, address, email address (including in a business context, email addresses of Individuals in companies such as `firstname.surname@organisation.com`), IP address and also more sensitive types of data such as trade union membership, genetic data and religious beliefs. These more sensitive types of data are called “Special Categories of Personal Data” and are defined below. Special Categories of Personal Data are given extra protection by Data Protection Laws.

**3.11. Processor** – Any entity (e.g. company, organisation or person) which accesses or uses Personal Data on the instruction of a Controller.

A Processor is a third party that processes Personal Data on behalf of a Controller. This is usually as a result of the outsourcing of a service by the Controller or the provision of services by the Processor which involve access to or use of Personal Data. Examples include: where software support for a system, which contains Personal Data, is provided by someone outside the business; cloud arrangements; and mail fulfilment services.

**3.12. Special Categories of Personal Data** – Personal Data that reveals a person’s racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data (i.e. information about their inherited or acquired genetic characteristics), biometric data (i.e. information about their physical, physiological or behavioral characteristics such as facial images and fingerprints), physical or mental health, sexual life or sexual orientation and criminal record. Special Categories of Personal Data are subject to additional controls in comparison to ordinary Personal Data.

#### **4. EFI GROUP PERSONNEL’S GENERAL OBLIGATIONS**

4.1. All EFI Group, subsidiary companies or business unit Personnel must comply with this policy.

4.2. All EFI Group and subsidiary company Personnel must ensure that they keep confidential all Personal Data that they collect, store, use and come into contact with during the performance of their duties.

4.3. All EFI Group and subsidiary company Personnel must not release or disclose any Personal Data:

4.3.1. outside the EFI Group; or

4.3.2. inside the EFI Group to all EFI Group and subsidiary company Personnel not authorised to access the Personal Data,

Without specific authorisation from their manager or the Data Protection Officer, this includes by phone calls or in emails.

4.4. All EFI Group and subsidiary company Personnel must take all steps to ensure there is no unauthorised access to Personal Data, whether by other EFI Group or subsidiary company Personnel who are not authorised to see such Personal Data, or by people outside of EFI Group.

#### **5. DATA PROTECTION PRINCIPLES**

5.1. When using Personal Data, Data Protection Laws require that the EFI Group and subsidiary companies comply with the following principles. These principles require Personal Data to be:

- 5.1.1. processed lawfully, fairly and in a transparent manner;
  - 5.1.2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
  - 5.1.3. adequate, relevant and limited to what is necessary for the purposes for which it is being processed;
  - 5.1.4. accurate and kept up to date, meaning that every reasonable step must be taken to ensure that Personal Data that is inaccurate is erased or rectified as soon as possible;
  - 5.1.5. kept for no longer than is necessary for the purposes for which it is being processed; and
  - 5.1.6. 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.
- 5.2. These principles are considered in more detail in the remainder of this Policy.
- 5.3. In addition to complying with the above requirements the EFI Group and subsidiary companies also have to demonstrate in writing that they comply with them. The EFI Group has a number of policies and procedures in place, including this Policy and the documentation referred to in it, to ensure that the EFI Group and subsidiary companies can demonstrate their compliance.

## **6. LAWFUL USE OF PERSONAL DATA**

- 6.1. In order to collect and/or use Personal Data lawfully the EFI Group and subsidiary companies need to be able to show that its use meets one of a number of legal grounds. Please click here to see the detailed grounds [<https://ico.org.uk/fororganisations/guide-to-the-general-data-protection-regulation-gdpr/lawfulbasis-for-processing>]
- 6.2. In addition, when the EFI Group and subsidiary companies collect and/or use Special Categories of Personal Data, the EFI Group or subsidiary company has to show that one of a number of additional conditions is met. Please click here to see the detailed additional conditions [<https://ico.org.uk/for-organisations/guide-to-the-generaldata-protection-regulation-gdpr/lawful-basis-for-processing/special-categorydata/>]
- 6.3. The EFI Group has carefully assessed how it uses Personal Data and how it complies with the obligations set out in paragraphs 6.1 and 6.2. If the EFI Group or subsidiary

companies change how they use Personal Data, EFI Group needs to update this record and may also need to notify Individuals about the change. If EFI Group or subsidiary company Personnel therefore intend to change how they use Personal Data at any point, they must notify the Data Protection Officer who will decide whether their intended use requires amendments to be made and any other controls which need to apply.

## **7. TRANSPARENT PROCESSING – PRIVACY NOTICES**

7.1. Where the EFI Group and subsidiary companies collect Personal Data directly from Individuals, the EFI Group or subsidiary company will inform them about how the organisation uses their Personal Data. This is detailed in each company's privacy notice. The EFI Group has adopted the following privacy notices:

- Staffing privacy notice provided by HR on joining can be found on **Staffology** and the **FRA SharePoint intranet hub ('FRamily home')**.
- The EFI Group Student privacy notice (named FRA Student Privacy Notice) can be found on the **FRA SharePoint intranet hub ('FRamily home')** under the Policy section, or the Fashion Retail Academy website.

7.2. If the EFI Group or any of the subsidiary companies receive Personal Data about an Individual from other sources, the EFI Group or subsidiary company will provide the Individual with a privacy notice about how the organisation will use their Personal Data. This will be provided as soon as reasonably possible and in any event within one month.

7.3. If the EFI Group or subsidiary company changes how it uses Personal Data, the organisation may need to notify Individuals about the change. If EFI Group or subsidiary company Personnel therefore intend to change how they use Personal Data please notify the EFI Group Data Protection Officer, or company specific Data Protection Officer, who will decide whether the organisation Personnel's intended use requires amendments to be made to the privacy notices and any other controls, which need to apply.

## **8. DATA QUALITY – ENSURING THE USE OF ACCURATE, UP TO DATE AND RELEVANT PERSONAL DATA**

8.1. Data Protection Laws require that the EFI Group and subsidiary companies only collect and process Personal Data to the extent that it is required for the specific purpose(s) notified to the Individual in a privacy notice (see paragraph 7 above) and as set out in the EFI Group or subsidiary company's record of how it uses Personal Data. The EFI Group and subsidiary companies are also required to ensure that the Personal Data the EFI Group or subsidiary company holds are accurate and kept up to date.

- 8.2. All EFI Group and subsidiary company Personnel that collect and record Personal Data shall ensure that the Personal Data is recorded accurately, is kept up to date and shall also ensure that they limit the collection and recording of Personal Data to that which is adequate, relevant and limited to what is necessary in relation to the purpose for which it is collected and used.
- 8.3. All EFI Group and subsidiary company Personnel that obtain Personal Data from sources outside the organisation shall take reasonable steps to ensure that the Personal Data is recorded accurately, is up to date and limited to that which is adequate, relevant and limited to what is necessary in relation to the purpose for which it is collected and used. This does not require the EFI Group or subsidiary company Personnel to independently check the Personal Data obtained.
- 8.4. In order to maintain the quality of Personal Data, all EFI Group and subsidiary company Personnel that access Personal Data shall ensure that they review, maintain and update it to ensure that it remains accurate, up to date, adequate, relevant and limited to what is necessary in relation to the purpose for which it is collected and used. Please note that this does not apply to Personal Data which the EFI Group or subsidiary company must keep in its original form (e.g. for legal reasons or that which is relevant to an investigation).
- 8.5. The EFI Group recognises the importance of ensuring that Personal Data is amended, rectified, erased or its use restricted where this is appropriate under Data Protection Laws. The Fashion Retail Academy has a Rights of Individuals Policy and a Rights of Individuals Procedure, which set out how the organisation responds to requests relating to these issues. Any request from an individual for the amendment, rectification, erasure or restriction of the use of their Personal Data should be dealt with in accordance with those documents.

## **9. PERSONAL DATA MUST NOT BE KEPT FOR LONGER THAN NEEDED**

- 9.1. Data Protection Laws require that the EFI Group and subsidiary companies do not keep Personal Data longer than is necessary for the purpose or purposes for which the EFI Group or the subsidiary company collected it.
- 9.2. The EFI Group has assessed the types of Personal Data that it holds and the purposes it uses it for and has set retention periods for the different types of Personal Data processed by the EFI Group, the reasons for those retention periods and how the EFI Group securely deletes Personal Data at the end of those periods. These are set out in the Data Retention Policy.
- 9.3. If EFI Group or subsidiary company Personnel feel that a particular item of Personal Data needs to be kept for more or less time than the retention period set out in the Data Retention Policy, for example because there is a requirement of law, or if EFI Group or subsidiary company Personnel have any questions about this Policy or the EFI Group's Personal Data retention practices, they should contact the Data Protection Officer for guidance.



## 10. DATA SECURITY

The EFI Group takes information security very seriously and the EFI Group has security measures against unlawful or unauthorised processing of Personal Data and against the accidental loss of, or damage to, Personal Data. The EFI Group has in place procedures and technologies to maintain the security of all Personal Data from the point of collection to the point of destruction.

## 11. DATA BREACH

### Training

11.1. Whilst the EFI Group takes information security very seriously, unfortunately, in today's environment, it is possible that a security breach could happen which may result in the unauthorised loss of, access to, deletion of or alteration of Personal Data. If this happens there will be a Personal Data breach and EFI Group or subsidiary company Personnel must comply with the EFI Group's Data Breach Notification Policy. Please see paragraphs 11.2 and 11.3 for examples of what can be a Personal Data breach. Please familiarise yourself with it as it contains important obligations which EFI Group and subsidiary company Personnel need to comply with in the event of Personal Data breaches.

11.2. Personal Data breach is defined very broadly and is effectively any failure to keep Personal Data secure, which leads to the accidental or unlawful loss (including loss of access to), destruction, alteration or unauthorised disclosure of Personal Data. Whilst most Personal Data breaches happen as a result of action taken by a third party, they can also occur as a result of something someone internal does.

11.3. There are three main types of Personal Data breach which are as follows:

11.3.1. **Confidentiality breach** - where there is an unauthorised or accidental disclosure of, or access to, Personal Data e.g. hacking, accessing internal systems that a EFI Group or subsidiary company Personnel is not authorised to access, accessing Personal Data stored on a lost laptop, phone or other device, people deceitfully obtaining access to Personal Data they have no right to access, putting the wrong letter in the wrong envelope, sending an email to the wrong individual, or disclosing information over the phone to the wrong individual.

11.3.2. **Availability breach** - where there is an accidental or unauthorised loss of access to, or destruction of, Personal Data e.g. loss of a memory stick, laptop or device, denial of service attack, infection of systems by ransom ware, deleting Personal Data in error, loss of access to Personal Data stored on systems, inability to restore access to Personal Data from back up, or loss of an encryption key; and

11.3.3. **Integrity breach** - where there is an unauthorised or accidental alteration of Personal Data.

## **12. APPOINTING CONTRACTORS WHO ACCESS THE EFI GROUP OR SUBSIDIARY COMPANY PERSONAL DATA**

12.1. If the EFI Group or subsidiary company appoints a contractor who is a Processor of the organization's Personal Data, Data Protection Laws require that the organisation only appoints them where they have carried out sufficient due diligence and only where the EFI Group or subsidiary company has appropriate contracts in place.

12.2. One requirement of GDPR is that a Controller must only use Processors who meet the requirements of the GDPR and protect the rights of individuals. This means that data protection due diligence should be undertaken on both new and existing suppliers. Once a Processor is appointed they should be audited periodically to ensure that they are meeting the requirements of their contract in relation to Data Protection.

12.3. Any contract where an organisation appoints a Processor must be in writing.

12.4. You are considered as having appointed a Processor where you engage someone to perform a service for you and as part of it they may get access to your Personal Data. Where you appoint a Processor you, as Controller remain responsible for what happens to the Personal Data.

12.5. GDPR requires the contract with a Processor to contain the following obligations as a minimum:

12.5.1. to only act on the written instructions of the Controller;

12.5.2. to not export Personal Data without the Controller's instruction;

12.5.3. to ensure staff are subject to confidentiality obligations;

12.5.4. to take appropriate security measures;

12.5.5. to only engage sub-processors with the prior consent (specific or general) of the Controller and under a written contract;

12.5.6. to keep the Personal Data secure and assist the Controller to do so;

12.5.7. to assist with the notification of Data Breaches and Data Protection Impact Assessments;

12.5.8. to assist with subject access/individuals rights;

12.5.9. to delete/return all Personal Data as requested at the end of the contract;

12.5.10. to submit to audits and provide information about the processing; and

12.5.11. to tell the Controller if any instruction is in breach of the GDPR or other EU or member state data protection law.

12.6. In addition the contract should set out:

12.6.1. The subject-matter and duration of the processing;

12.6.2. the nature and purpose of the processing;

12.6.3. the type of Personal Data and categories of individuals; and

12.6.4. the obligations and rights of the Controller.

### **13. INDIVIDUALS' RIGHTS**

13.1. GDPR gives individuals more control about how their data is collected and stored and what is done with it. Some existing rights of individuals have been expanded upon and some new rights have been introduced. It is extremely important that the EFI Group plans how they will handle these requests under GDPR.

13.2. The different types of rights of individuals are reflected in this paragraph.

#### **13.3. Subject Access Requests**

13.3.1. Individuals have the right under the GDPR to ask the EFI Group or its subsidiary companies to confirm what Personal Data they hold in relation to them and provide them with the data. This is not a new right, but additional information has to be provided, and the timescale for providing it has now been reduced from 40 days to one month (with a possible extension if it is a complex request). In addition, the organisation responding to the Subject Access Request will no longer be able to charge a fee for complying with the request.

13.3.2. Subject Access Requests are becoming more and more common and are often made in the context of a dispute which means that it is crucial that they are handled appropriately to avoid a complaint being made to the ICO.

#### **13.4. Right of Erasure (Right to be Forgotten)**

13.4.1. This is a limited right for individuals to request the erasure of Personal Data concerning them where:

13.4.1.1. the use of the Personal Data is no longer necessary;

13.4.1.2. their consent is withdrawn and there is no other legal ground for the processing;

13.4.1.3. the individual objects to the processing and there are no overriding legitimate grounds for the processing;

13.4.1.4. the Personal Data has been unlawfully processed; and

13.4.1.5. the Personal Data has to be erased for compliance with a legal obligation.

13.4.2. In a marketing context, where Personal Data is collected and processed for direct marketing purposes, the individual has a right to object to processing at any time. Where the individual objects, the Personal Data must not be processed for such purposes.

### **13.5. Right of Data Portability**

13.5.1. An individual has the right to request that data concerning them is provided to them in a structured, commonly used and machine-readable format where:

13.5.1.1. the processing is based on consent or on a contract; and

13.5.1.2. the processing is carried out by automated means

13.5.2. This right is not the same as subject access and is intended to give individuals a subset of their data.

### **13.6. The Right of Rectification and Restriction**

13.6.1. Finally, individuals are also given the right to request that any Personal Data is rectified if inaccurate and to have use of their Personal Data restricted to particular purposes in certain circumstances.

13.7. The EFI Group and subsidiary companies will use all Personal Data in accordance with the rights given to Individuals' under Data Protection Laws, and will ensure that it allows Individuals to exercise their rights in accordance with the EFI Group's Rights of Individuals Policy and Rights of Individuals Procedure. Please familiarise yourself with these documents as they contain important obligations which EFI Group and subsidiary company Personnel need to comply with in relation to the rights of Individuals over their Personal Data.

## **14. MARKETING AND CONSENT**

14.1. The EFI Group or subsidiary companies will sometimes contact Individuals to send them marketing or to promote the EFI Group or the relevant subsidiary company. Where the EFI Group or subsidiary company carries out any marketing, Data Protection Laws require that this is only done in a legally compliant manner.

14.2. Marketing consists of any advertising or marketing communication that is directed to particular individuals. GDPR will bring about a number of important changes for organisations that market to individuals, including:

- 14.2.1. providing more detail in their privacy notices, including for example whether profiling takes place; and
- 14.2.2. rules on obtaining consent will be stricter and will require an individual's "clear affirmative action". The ICO like consent to be used in a marketing context.
- 14.3. EFI Group and its subsidiary companies also need to be aware of the Privacy and Electronic Communications Regulations (PECR) that sit alongside data protection. PECR apply to direct marketing i.e. a communication directed to particular individuals and covers any advertising/marketing material. It applies to electronic communication i.e. calls, emails, texts, faxes. PECR rules apply even if you are not processing any personal data
- 14.4. Consent is central to electronic marketing. We would recommend that best practice is to provide an un-ticked opt-in box.
- 14.5. Alternatively, the EFI Group or subsidiary company may be able to market using a "soft opt in" if the following conditions were met:
  - 14.5.1. contact details have been obtained in the course of a sale (or negotiations for a sale);
  - 14.5.2. the EFI Group or subsidiary company are marketing its own similar services; and
  - 14.5.3. the EFI Group or subsidiary company gives the individual a simple opportunity to opt out of the marketing, both when first collecting the details and in every message after that.

## 15. AUTOMATED DECISION MAKING AND PROFILING

15.1. Under Data Protection Laws there are controls around profiling and automated decision making in relation to Individuals.

**Automated Decision Making** happens where the EFI Group or subsidiary company makes a decision about an Individual solely by automated means without any human involvement and the decision has legal or other significant effects; and

**Profiling** happens where the EFI Group or subsidiary company automatically uses Personal Data to evaluate certain things about an Individual.

15.2. Any Automated Decision Making or Profiling which the EFI Group or subsidiary companies carry out can only be done once the organisation is confident that it is complying with Data Protection Laws. If EFI Group or subsidiary company Personnel therefore wish to carry out any Automated Decision Making or Profiling, Personnel must inform the Data Protection Officer before doing so.

15.3. EFI Group or subsidiary company Personnel must not carry out Automated Decision Making or Profiling without the approval of the Data Protection Officer.

15.4. The EFI Group or subsidiary companies do not carry out Automated Decision Making or Profiling in relation to its employees.

## **16. DATA PROTECTION IMPACT ASSESSMENTS (DPIA)**

16.1. The GDPR introduce a new requirement to carry out a risk assessment in relation to the use of Personal Data for a new service, product or process. This must be done prior to the processing via a Data Protection Impact Assessment (“**DPIA**”). A DPIA should be started as early as practical in the design of processing operations. A DPIA is not a prohibition on using Personal Data but is an assessment of issues affecting Personal Data which need to be considered before a new product/service/process is rolled out. The process is designed to:

16.1.1. describe the collection and use of Personal Data;

16.1.2. assess its necessity and its proportionality in relation to the purposes;

16.1.3. assess the risks to the rights and freedoms of individuals; and

16.1.4. the measures to address the risks.

16.2. A DPIA must be completed where the use of Personal Data is likely to result in a high risk to the rights and freedoms of individuals.

16.3. Where a DPIA reveals risks which are not appropriately mitigated the ICO must be consulted.

16.4. Where the EFI Group or subsidiary companies are launching or proposing to adopt a new process, product or service which involves Personal Data, the organisation needs to consider whether it needs to carry out a DPIA as part of the project initiation process. The organisation needs to carry out a DPIA at an early stage in the process so that the EFI Group or subsidiary company can identify and fix problems with its proposed new process, product or service at an early stage, reducing the associated costs and damage to reputation, which might otherwise occur.

16.5. Situations where the EFI Group or subsidiary company may have to carry out a Data Protection Impact Assessment include the following (please note that this list is not exhaustive):

16.5.1. large scale and systematic use of Personal Data for the purposes of Automated Decision Making or Profiling (see definitions above) where legal or similarly significant decisions are made;

16.5.2. large scale use of Special Categories of Personal Data, or Personal Data relating to criminal convictions and offences e.g. the use of high volumes of health data; or

16.5.3. systematic monitoring of public areas on a large scale e.g. CCTV cameras.

16.6. All DPIAs must be reviewed and approved by the Data Protection Officer.

## **17. TRANSFERRING PERSONAL DATA TO A COUNTRY OUTSIDE THE EEA**

17.1. Data Protection Laws impose strict controls on Personal Data being transferred outside the EEA. Transfer includes sending Personal Data outside the EEA but also includes storage of Personal Data or access to it outside the EEA. It needs to be thought about whenever the EFI Group or subsidiary company appoints a supplier outside the EEA, or the EFI Group or subsidiary company appoints a supplier with group companies outside the EEA which may give access to the Personal Data to staff outside the EEA.

17.2. So that the EFI Group and its subsidiary companies can ensure they are compliant with Data Protection Laws, Personnel must not export Personal Data unless it has been approved by the Data Protection Officer.

17.3. EFI Group or subsidiary company Personnel must not export any Personal Data outside the EEA without the approval of the Data Protection Officer.

## **18. CCTV**

18.1 The EFI Group utilises Closed Circuit Televisions (CCTV) on an evidentiary basis when incidents of crime or misconduct have been alleged. CCTV data is held securely for 30 days before being permanently erased. The data is sealed, and only authorised individuals may be able to view the data. Permission must be sought and granted from the EFI Group or company's Data Protection Officer before any downloads can take place.

## **19. Training**

19.1 Training will be provided to all EFI Group Personnel to ensure that they are informed of their responsibilities, however as referenced above it is the responsibility of staff to ensure that they conduct themselves in line with this policy (4 General Obligations). All newly appointed EFI Group or subsidiary company Personnel will be required to complete a data protection training module as part of the onboarding process.