Reference	GDPR 01
Version	2.0
Issue Date	19.03.20
Approved	Mark White
Review on	19.09.20

DIRECT FLAME LTD

GDPR POLICY – DATA HANDLING

GDPR Manual

Company ICO Number

ZA326727

Reference	GDPR 01
Version	2.0
Issue Date	19.03.20
Approved	Mark White
Review on	19.09.20

DIRECT FLAME LTD

GDPR POLICY – DATA HANDLING

Table of Contents

Reference	GDPR 01
Version	2.0
Issue Date	19.03.20
Approved	Mark White
Review on	19.09.20

DIRECT FLAME LTD

GDPR POLICY – DATA HANDLING

1. Introduction

Direct Flame Ltd is committed to conducting its business in accordance with all applicable Data Protection laws and regulations and in line with the highest standards of ethical conduct.

This policy sets forth the expected behaviours of Direct Flame Ltd Employees and Third Parties in relation to the collection, use, retention, transfer, disclosure and destruction of any Personal Data belonging to a Direct Flame Ltd Contact (i.e. the Data Subject).

Personal Data is any information (including opinions and intentions) which relates to an identified or Identifiable Natural Person. Personal Data is subject to certain legal safeguards and other regulations, which impose restrictions on how organisations may process Personal Data. An organisation that handles Personal Data and makes decisions about its use is known as a Data Controller. Direct Flame Ltd, as a Data Controller, is responsible for ensuring compliance with the Data Protection requirements outlined in this policy. Non-compliance may expose Direct Flame Ltd to complaints, regulatory action, fines and/or reputational damage.

Direct Flame Ltd's leadership is fully committed to ensuring continued and effective implementation of this policy and expects all Direct Flame Ltd Employees and Third Parties to share in this commitment. Any breach of this policy will be taken seriously and may result in disciplinary action or business sanction.

This policy has been approved by Direct Flame Ltd's Managing Director

2. Scope

This policy applies to all Direct Flame Ltd Entities where a Data Subject's Personal Data is processed:

- In the context of the business activities of the Direct Flame Ltd Entity.
- For the provision or offer of goods or services to individuals (including those provided or offered free-of-charge) by a Direct Flame Ltd Entity.
- To actively monitor the behaviour of individuals.
- Monitoring the behaviour of individuals includes using data processing techniques such as persistent web browser cookies or dynamic IP address tracking to profile an individual with a view to:
- Taking a decision about them.
- Analysing or predicting their personal preferences, behaviours and attitudes.

This policy applies to all Processing of Personal Data in electronic form (including electronic mail and documents created with word processing software) or where it is held in manual files that are structured in a way that allows ready access to information about individuals.

This policy has been designed to establish a worldwide baseline standard for the Processing and protection of Personal Data by all Direct Flame Ltd Entities. Where national law imposes a requirement, which is stricter than imposed by this policy, the requirements in national law must be

followed. Furthermore, where national law imposes a requirement that is not addressed in this policy, the relevant national law must be adhered to.

If there are conflicting requirements in this policy and national law, please consult with Office of Data Protection for guidance.

The protection of Personal Data belonging to Direct Flame Ltd Employees is not within the scope of this policy. It is covered in the Direct Flame Ltd 'Data Protection for Employee Data' policy.

3. Definitions

Employee: An individual who works part-time or full-time for Direct Flame Ltd under a contract of employment, whether oral or written, express or implied, and has recognised rights and duties. Includes temporary employees and independent contractors.

Third Party: An external organisation with which Direct Flame Ltd conducts business and is also authorised to, under the direct authority of Direct Flame Ltd, Process the Personal Data of Direct Flame Ltd Contacts.

Personal Data: Any information (including opinions and intentions) which relates to an identified or Identifiable Natural Person.

Contact any past, current or prospective Direct Flame Ltd customer.

Identifiable Natural Person: Anyone who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Data Controller: A natural or legal person, Public Authority, Agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

Direct Flame Ltd Entity: A Direct Flame Ltd establishment, including subsidiaries and joint ventures over which Direct Flame Ltd exercise management control.

Data Subject: The identified or Identifiable Natural Person to which the data refers.

Process, Processed, Processing: Any operation or set of operations performed on personal Data or on sets of Personal Data, whether or not by automated means. Operations performed may include collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Data Protection: The process of safeguarding Personal Data from unauthorised or unlawful disclosure, access, alteration, Processing, transfer or destruction.

Data Protection Authority: An independent Public Authority responsible for monitoring the application of the relevant Data Protection regulation set forth in national law.

Data Processors: A natural or legal person, Public Authority, Agency or other body which Processes Personal Data on behalf of a Data controller.

Consent: Any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the Processing of Personal Data relating to him or her.

Special Categories of Data: Personal Data pertaining to or revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership; data concerning health or sex life and sexual orientation; genetic data or biometric data.

Third Country: Any country not recognised as having an adequate level of legal protection for the rights and freedoms of Data Subjects in relation to the Processing of Personal Data.

Profiling: Any form of automated processing of Personal Data where Personal Data is used to evaluate specific or general characteristics relating to an Identifiable Natural Person. In particular to analyse or predict certain aspects concerning that natural person's performance at work, economic situations, health, personal preferences, interests, reliability, behaviour, location or movement.

Binding Corporate Rules: The Personal Data protection policies used for the transfer of Personal Data to one or more Third Countries within a group of undertakings, or group of enterprises engaged in a joint economic activity.

Personal Data Breach: A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed.

Encryption: The process of converting information or data into code, to prevent unauthorised access.

Pseudonymisation: Data amended in such a way that no individuals can be identified from the data (whether directly or indirectly) without a "key" that allows the data to be re-identified.

Anonymisation: Data amended in such a way that no individuals can be identified from the data (whether directly or indirectly) by any means or by any person.

4. Policy

4.1 Governance

4.1.1 Office of Data Protection

To demonstrate our commitment to Data Protection, and to enhance the effectiveness of our compliance efforts, Direct Flame Ltd has established an Office of Data Protection. The Office operates with independence and is staffed by suitability skilled individuals granted all necessary authority. The Office of Data Protection reports to Direct Flame Ltd's Chief Risk Officer who has direct access to the Direct Flame Ltd Board of Directors. The Office of Data Protection includes regional Data Protection Officers (DPOs) whose duties include:

• Informing and advising Direct Flame Ltd and its Employees who carry out Processing pursuant to Data Protection regulations, national law or Union based Data Protection provisions;

• Ensuring the alignment of this policy with Data Protection regulations, national law or Union based Data Protection provisions;

• Providing guidance with regards to carrying out Data Protection Impact Assessments (DPIAs);

• Acting as a point of contact for and cooperating with Data Protection Authorities (DPAs);

• Determining the need for notifications to one or more DPAs as a result of Direct Flame Ltd's current or intended Personal Data processing activities;

• Making and keeping current notifications to one or more DPAs as a result of Direct Flame Ltd's current or intended Personal Data processing activities;

• The establishment and operation of a system providing prompt and appropriate responses to Data Subject requests;

4.1.1 Office of Data Protection (Cont.)

• Informing senior managers, officers, and directors of Direct Flame Ltd of any potential corporate, civil and criminal penalties which may be levied against Direct Flame Ltd and/or its Employees for violation of applicable Data Protection laws.

• Ensuring establishment of procedures and standard contractual provisions for obtaining compliance with this Policy by any Third Party who:

• provides Personal Data to a Direct Flame Ltd Entity

• receives Personal Data from a Direct Flame Ltd Entity

• has access to Personal Data collected or processed by a Direct Flame Ltd Entity.

4.1.2 Policy Dissemination & Enforcement

The management team of each Direct Flame Ltd Entity must ensure that all Direct Flame Ltd Employees responsible for the Processing of Personal Data are aware of and comply with the contents of this policy.

In addition, each Direct Flame Ltd Entity will make sure all Third Parties engaged to Process Personal Data on their behalf (i.e. their Data Processors) are aware of and comply with the contents of this policy. Assurance of such compliance must be obtained from all Third Parties, whether companies or individuals, prior to granting them access to Personal Data controlled by Direct Flame Ltd.

4.1.3 Data Protection by Design

To ensure that all Data Protection requirements are identified and addressed when designing new systems or processes and/or when reviewing or expanding existing systems or processes, each of them must go through an approval process before continuing.

Each Direct Flame Ltd Entity must ensure that a Data Protection Impact Assessment (DPIA) is conducted, in cooperation with the Office of Data Protection, for all new and/or revised systems or processes for which it has responsibility. The subsequent findings of the DPIA must then be submitted to the Chief Risk Officer for review and approval. Where applicable, the Information

Technology (IT) department, as part of its IT system and application design review process, will cooperate with the Office of Data Protection to assess the impact of any new technology uses on the security of Personal Data.

4.1.4 Compliance Monitoring

To confirm that an adequate level of compliance that is being achieved by all Direct Flame Ltd Entities in relation to this policy, the Office of Data Protection will carry out an annual Data Protection compliance audit for all such Entities. Each audit will, as a minimum, assess:

• Compliance with Policy in relation to the protection of Personal Data, including:

• The assignment of responsibilities.

• Raising awareness.

• Training of Employees.

• The effectiveness of Data Protection related operational practices, including:

• Data Subject rights.

• Personal Data transfers.

• Personal Data incident management.

• Personal Data complaints handling.

• The level of understanding of Data Protection policies and Privacy Notices.

• The currency of Data Protection policies and Privacy Notices.

• The accuracy of Personal Data being stored.

•The conformity of Data Processor activities.

•The adequacy of procedures for redressing poor compliance and Personal Data Breaches.

The Office of Data Protection, in cooperation with key business stakeholders from each Direct Flame Ltd Entity, will devise a plan with a schedule for correcting any identified deficiencies within a defined and reasonable time frame. Any major deficiencies identified will be reported to and monitored by the Direct Flame Ltd Executive Management team.

4.2 Data Protection Principles

Direct Flame Ltd has adopted the following principles to govern its collection, use, retention, transfer, disclosure and destruction of Personal Data:

• Principle 1: Lawfulness, Fairness and Transparency

Personal Data shall be processed lawfully, fairly and in a transparent manner in relation to the Data Subject. This means, Direct Flame Ltd must tell the Data Subject what Processing will occur (transparency), the Processing must match the description given to the Data Subject (fairness), and it must be for one of the purposes specified in the applicable Data Protection regulation (lawfulness).

4.2 Data Protection Principles

• Principle 2: Purpose Limitation

Personal Data shall be collected for specified, explicit and legitimate purposes and not further Processed in a manner that is incompatible with those purposes. This means Direct Flame Ltd must specify exactly what the Personal Data collected will be used for and limit the Processing of that Personal Data to only what is necessary to meet the specified purpose.

• Principle 3: Data Minimisation

Personal Data shall be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are Processed. This means Direct Flame Ltd must not store any Personal Data beyond what is strictly required.

• Principle 4: Accuracy

Personal Data shall be accurate and, kept up to date.

This means Direct Flame Ltd must have in place processes for identifying and addressing out-of-date, incorrect, and redundant Personal Data.

• Principle 5: Storage Limitation

Personal Data shall be kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data is Processed. This means Direct Flame Ltd must, wherever possible, store Personal Data in a way that limits or prevents identification of the Data Subject.

• Principle 6: Integrity & Confidentiality

Personal Data shall be 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. Direct Flame Ltd must use appropriate technical and organisational measures to ensure the integrity and confidentiality of Personal Data is maintained at all times.

4.2 Data Protection Principles

• Principle 7: Accountability

The Data Controller shall be responsible for, and be able to demonstrate compliance. This means Direct Flame Ltd must demonstrate that the six Data Protection Principles (outlined above) are met for all Personal Data for which it is responsible.

4.3 Data Collection

4.3.1 Data Sources

Personal Data should be collected only from the Data Subject unless one of the following apply:

• The nature of the business purpose necessitates collection of the Personal Data from other persons or bodies.

• The collection must be carried out under emergency circumstances in order to protect the vital interests of the Data Subject or to prevent serious loss or injury to another person.

If Personal Data is collected from someone other than the Data Subject, the Data Subject must be informed1 of the collection unless one of the following apply:

• The Data Subject has received the required information by other means.

• The information must remain confidential due to a professional secrecy obligation

• A national law expressly provides for the collection, processing or transfer of the Personal Data.

Where it has been determined that notification to a Data Subject is required, notification should occur promptly, but in no case later than:

• One calendar month from the first collection or recording of the Personal Data

• At the time of first communication if used for communication with the Data Subject

• At the time of disclosure if disclosed to another recipient.

4.3.2 Data Subject Consent

Each Direct Flame Ltd Entity will obtain Personal Data only by lawful and fair means and, where appropriate with the knowledge and Consent of the individual concerned. Where a need exists to request and receive the Consent of an individual prior to the collection, use or disclosure of their Personal Data, Direct Flame Ltd is committed to seeking such Consent.

The Office of Data Protection, in cooperation with Group General Counsel, the Chief Risk Officer, the Chief Information Security Officer, the Chief Information Officer, and other relevant business representatives, shall establish a system for obtaining and documenting Data Subject Consent for the collection, Processing, and/or transfer of their Personal Data. The system must include provisions for:

• Determining what disclosures should be made in order to obtain valid Consent.

• Ensuring the request for consent is presented in a manner which is clearly distinguishable from any other matters, is made in an intelligible and easily accessible form, and uses clear and plain language.

• Ensuring the Consent is freely given (i.e. is not based on a contract that is conditional to the Processing of Personal Data that is unnecessary for the performance of that contract).

• Documenting the date, method and content of the disclosures made, as well as the validity, scope, and volition of the Consents given.

• Providing a simple method for a Data Subject to withdraw their Consent at any time.

4.3.3 Data Subject Notification

Each Direct Flame Ltd Entity will, when required by applicable law, contract, or where it considers that it is reasonably appropriate to do so, provide Data Subjects with information as to the purpose of the Processing of their Personal Data.

When the Data Subject is asked to give Consent to the Processing of Personal Data and when any Personal Data is collected from the Data Subject, all appropriate disclosures2 will be made, in a manner that draws attention to them, unless one of the following apply:

• The Data Subject already has the information

• A legal exemption applies to the requirements for disclosure and/or Consent.

The disclosures may be given orally, electronically or in writing. If given orally, the person making the disclosures should use a suitable script or form approved in advance by the Office of Data Protection. The associated receipt or form should be retained, along with a record of the facts, date, content, and method of disclosure.

4.3.4 External Privacy Notices

Each external website provided by a Direct Flame Ltd Entity will include an online 'Privacy Notice' and an online 'Cookie Notice' fulfilling the requirements of applicable law. Refer to Direct Flame Ltd's 'Internet Privacy Notice' and 'Internet Cookie Notice' standard templates for guidance. All Privacy and Cookie Notices must be approved by the Office of Data Protection prior to publication on any Direct Flame Ltd external website.

4.4 Data Use

4.4.1 Data Processing

Direct Flame Ltd uses the Personal Data of its Contacts for the following broad purposes:

• The general running and business administration of Direct Flame Ltd Entities.

• To provide services to Direct Flame Ltd customers.

• The ongoing administration and management of customer services.

The use of a Contact's information should always be considered from their perspective and whether the use will be within their expectations or if they are likely to object. For example, it would clearly be within a Contact's expectations that their details will be used by Direct Flame Ltd to respond to a Contact request for information about the products and services on offer. However, it will not be within their reasonable expectations that Direct Flame Ltd would then provide their details to Third Parties for marketing purposes.

Each Direct Flame Ltd Entity will Process Personal Data in accordance with all applicable laws and applicable contractual obligations. More specifically, Direct Flame Ltd will not Process Personal Data unless at least one of the following requirements are met:

• The Data Subject has given Consent to the Processing of their Personal Data for one or more specific purposes.

• Processing is necessary for the performance of a contract to which the Data Subject is party or in order to take steps at the request of the Data Subject prior to entering into a contract.

• Processing is necessary for compliance with a legal obligation to which the Data Controller is subject.

• Processing is necessary in order to protect the vital interests of the Data Subject or of another natural person.

• Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Data Controller.

• Processing is necessary for the purposes of the legitimate interests pursued by the Data Controller or by a Third Party (except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject, in particular where the Data Subject is a child).

There are some circumstances in which Personal Data may be further processed for purposes that go beyond the original purpose for which the Personal Data was collected. When making a determination as to the compatibility of the new reason for Processing, guidance and approval must be obtained from the Office of Data Protection before any such Processing may commence.

4.4.1 Data Processing

In any circumstance where Consent has not been gained for the specific Processing in question, Direct Flame Ltd will address the following additional conditions to determine the fairness and transparency of any Processing beyond the original purpose for which the Personal Data was collected:

• Any link between the purpose for which the Personal Data was collected and the reasons for intended further Processing.

• The context in which the Personal Data has been collected, in particular regarding the relationship between Data Subject and the Data Controller.

• The nature of the Personal Data, in particular whether Special Categories of Data are being Processed, or whether Personal Data related to criminal convictions and offences are being Processed.

• The possible consequences of the intended further Processing for the Data Subject.

• The existence of appropriate safeguards pertaining to further Processing, which may include Encryption, Anonymisation or Pseudonymisation.

4.4.2 Special Categories of Data

Direct Flame Ltd will only Process Special Categories of Data (also known as sensitive data) where the Data Subject expressly consents to such Processing or where one of the following conditions apply:

• The Processing relates to Personal Data which has already been made public by the Data Subject.

• The Processing is necessary for the establishment, exercise or defence of legal claims.

• The Processing is specifically authorised or required by law.

• The Processing is necessary to protect the vital interests of the Data Subject or of another natural person where the Data Subject is physically or legally incapable of giving consent.

• Further conditions, including limitations, based upon national law related to the Processing of genetic data, biometric data or data concerning health.

4.4.2 Special Categories of Data

In any situation where Special Categories of Data are to be Processed, prior approval must be obtained from the Office of Data Protection and the basis for the Processing clearly recorded with the Personal Data in question.

Where Special Categories of Data are being Processed, Direct Flame Ltd will adopt additional protection measures. Each Direct Flame Ltd Entity may also adopt additional measures to address local custom or social expectation over the Processing of Special Categories of Data.

4.4.3 Children's Data

Children are unable to Consent to the Processing of Personal Data for information society services . Consent must be sought from the person who holds parental responsibility over the child. However, it should be noted that where Processing is lawful under other grounds, Consent need not be obtained from the child or the holder of parental responsibility.

Should any Direct Flame Ltd Entity foresee a business need for obtaining parental consent for information society services offered directly to a child, guidance and approval must be obtained from the Office of Data Protection before any Processing of a child's Personal Data may commence.

4.4.4 Data Quality

Each Direct Flame Ltd Entity will adopt all necessary measures to ensure that the Personal Data it collects and Processes is complete and accurate in the first instance, and is updated to reflect the current situation of the Data Subject.

The measures adopted by Direct Flame Ltd to ensure data quality include:

4.4.4 Data Quality

- Correcting Personal Data known to be incorrect, inaccurate, incomplete, ambiguous, misleading or outdated, even if the Data Subject does not request rectification.
- Keeping Personal Data only for the period necessary to satisfy the permitted uses or applicable statutory retention period.
- The removal of Personal Data if in violation of any of the Data Protection principles or if the Personal Data is no longer required.
- Restriction, rather than deletion of Personal Data, insofar as:

- a law prohibits erasure.
- erasure would impair legitimate interests of the Data Subject.
- the Data Subject disputes that their Personal Data is correct, and it cannot be clearly ascertained whether their information is correct or incorrect.

4.4.5 Profiling & Automated Decision-Making

Direct Flame Ltd will only engage in Profiling and automated decision-making where it is necessary to enter into, or to perform, a contract with the Data Subject or where it is authorised by law.

Where a Direct Flame Ltd Entity utilises Profiling and automated decision-making, this will be disclosed to the relevant Data Subjects. In such cases the Data Subject will be given the opportunity to:

• Express their point of view.

• Obtain an explanation for the automated decision.

• Review the logic used by the automated system.

• Supplement the automated system with additional data.

• Have a human carry out a review of the automated decision.

• Contest the automated decision.

• Object to the automated decision-making being carried out.

Each Direct Flame Ltd Entity must also ensure that all Profiling and automated decision-making relating to a Data Subject is based on accurate data.

4.4.6 Digital Marketing

As a general rule Direct Flame Ltd will not send promotional or direct marketing material to a Direct Flame Ltd Contact through digital channels such as mobile phones, email and the Internet, without first obtaining their Consent. Any Direct Flame Ltd Entity wishing to carry out a digital marketing campaign without obtaining prior Consent from the Data Subject must first have it approved by the Office of Data Protection.

Where Personal Data Processing is approved for digital marketing purposes, the Data Subject must be informed at the point of first contact that they have the right to object, at any stage, to having their data Processed for such purposes. If the Data Subject puts forward an objection, digital marketing related Processing of their Personal Data must cease immediately, and their details should be kept on a suppression list with a record of their opt-out decision, rather than being completely deleted.

It should be noted that where digital marketing is carried out in a 'business to business' context, there is no legal requirement to obtain an indication of Consent to carry out digital marketing to individuals provided that they are given the opportunity to opt-out.

4.5 Data Retention

To ensure fair Processing, Personal Data will not be retained by Direct Flame Ltd for longer than necessary in relation to the purposes for which it was originally collected, or for which it was further Processed.

The length of time for which Direct Flame Ltd Entities need to retain Personal Data is set out in the Direct Flame Ltd 'Personal Data Retention Schedule'. This takes into account the legal and contractual requirements, both minimum and maximum, that influence the retention periods set forth in the schedule. All Personal Data should be deleted or destroyed as soon as possible where it has been confirmed that there is no longer a need to retain it.

4.6 Data Protection

Each Direct Flame Ltd Entity will adopt physical, technical, and organisational measures to ensure the security of Personal Data. This includes the prevention of loss or damage, unauthorised alteration, access or Processing, and other risks to which it may be exposed by virtue of human action or the physical or natural environment.

The minimum set of security measures to be adopted by each Direct Flame Ltd Entity is provided in the Direct Flame Ltd 'Information Security Policy'. A summary of the Personal Data related security measures is provided below:

• Prevent unauthorised persons from gaining access to data processing systems in which Personal Data are Processed.

• Prevent persons entitled to use a data processing system from accessing Personal Data beyond their needs and authorisations.

• Ensure that Personal Data in the course of electronic transmission during transport cannot be read, copied, modified or removed without authorisation.

• Ensure that access logs are in place to establish whether, and by whom, the Personal Data was entered into, modified on or removed from a data processing system.

• Ensure that in the case where Processing is carried out by a Data

Processor, the data can be Processed only in accordance with the instructions of the Data Controller.

• Ensure that Personal Data is protected against undesired destruction or loss.

• Ensure that Personal Data collected for different purposes can and is Processed separately.

• Ensure that Personal Data is not kept longer than necessary.

4.7 Data Subject Requests

The Office of Data Protection will establish a system to enable and facilitate the exercise of Data Subject rights related to:

• Information access.

• Objection to Processing.

• Objection to automated decision-making and profiling.

• Restriction of Processing.

• Data portability.

• Data rectification.

• Data erasure.

If an individual makes a request relating to any of the rights listed above, Direct Flame Ltd will consider each such request in accordance with all applicable Data Protection laws and regulations. No administration fee will be charged for considering and/or complying with such a request unless the request is deemed to be unnecessary or excessive in nature.

Data Subjects are entitled to obtain, based upon a request made in writing to the Office of Data Protection and upon successful verification of their identity, the following information about their own Personal Data:

• The purposes of the collection, Processing, use and storage of their Personal Data.

• The source(s) of the Personal Data, if it was not obtained from the Data Subject;

• The categories of Personal Data stored for the Data Subject.

• The recipients or categories of recipients to whom the Personal Data has been or may be transmitted, along with the location of those recipients.

• The envisaged period of storage for the Personal Data or the rationale for determining the storage period.

• The use of any automated decision-making, including Profiling.

4.7 Data Subject Requests

• The right of the Data subject to:

• object to Processing of their Personal Data.

• lodge a complaint with the Data Protection Authority.

• request rectification or erasure of their Personal Data.

• request restriction of Processing of their Personal Data.

All requests received for access to or rectification of Personal Data must be directed to the Office of Data Protection, who will log each request as it is received. A response to each request will be provided within 30 days of the receipt of the written request from the Data Subject. Appropriate verification must confirm that the requestor is the Data Subject or their authorised legal

representative. Data Subjects shall have the right to require Direct Flame Ltd to correct or supplement erroneous, misleading, outdated, or incomplete Personal Data.

If Direct Flame Ltd cannot respond fully to the request within 30 days, the Office of Data Protection shall nevertheless provide the following information to the Data Subject, or their authorised legal representative within the specified time:

• An acknowledgement of receipt of the request.

• Any information located to date.

• Details of any requested information or modifications which will not be provided to the Data Subject, the reason(s) for the refusal, and any procedures available for appealing the decision.

• An estimated date by which any remaining responses will be provided.

• An estimate of any costs to be paid by the Data Subject (e.g. where the request is excessive in nature).

• The name and contact information of the Direct Flame Ltd individual who the Data Subject should contact for follow up.

4.7 Data Subject Requests

It should be noted that situations may arise where providing the information requested by a Data Subject would disclose Personal Data about another individual. In such cases, information must be redacted or withheld as may be necessary or appropriate to protect that person's rights.

Detailed guidance for dealing with requests from Data Subjects can be found in the Direct Flame Ltd 'Data Subject Request Handling Procedures' document.

4.8 Law Enforcement Requests & Disclosures

In certain circumstances, it is permitted that Personal Data be shared without the knowledge or Consent of a Data Subject. This is the case where the disclosure of the Personal Data is necessary for any of the following purposes:

• The prevention or detection of crime.

• The apprehension or prosecution of offenders.

• The assessment or collection of a tax or duty.

• By the order of a court or by any rule of law.

If a Direct Flame Ltd Entity Processes Personal Data for one of these purposes, then it may apply an exception to the Processing rules outlined in this policy but only to the extent that not doing so would be likely to prejudice the case in question.

If any Direct Flame Ltd Entity receives a request from a court or any regulatory or law enforcement authority for information relating to a Direct Flame Ltd Contact, you must immediately notify the Office of Data Protection who will provide comprehensive guidance and assistance.

4.9 Data Protection Training

All Direct Flame Ltd Employees that have access to Personal Data will have their responsibilities under this policy outlined to them as part of their staff induction training. In addition, each Direct Flame Ltd Entity will provide regular Data Protection training and procedural guidance for their staff.

The training and procedural guidance set forth will consist of, at a minimum, the following elements:

• The Data Protection Principles set forth in Section 4.2 above.

• Each Employee's duty to use and permit the use of Personal Data only by authorised persons and for authorised purposes.

• The need for, and proper use of, the forms and procedures adopted to implement this policy.

• The correct use of passwords, security tokens and other access mechanisms.

• The importance of limiting access to Personal Data, such as by using password protected screen savers and logging out when systems are not being attended by an authorised person.

• Securely storing manual files, print outs and electronic storage media.

• The need to obtain appropriate authorisation and utilise appropriate safeguards for all transfers of Personal Data outside of the internal network and physical office premises.

• Proper disposal of Personal Data by using secure shredding facilities.

• Any special risks associated with particular departmental activities or duties.

4.10 Data Transfers

Direct Flame Ltd Entities may transfer Personal Data to internal or Third-Party recipients located in another country where that country is recognised as having an adequate level of legal protection for the rights and freedoms of the relevant Data Subjects. Where transfers need to be made to countries lacking an adequate level of legal protection (i.e. Third Countries), they must be made in compliance with an approved transfer mechanism

Direct Flame Ltd Entities may only transfer Personal Data where one of the transfer scenarios list below applies:

• The Data Subject has given Consent to the proposed transfer.

• The transfer is necessary for the performance of a contract with the Data Subject.

• The transfer is necessary for the implementation of pre-contractual measures taken in response to the Data Subject's request.

• The transfer is necessary for the conclusion or performance of a contract concluded with a Third Party in the interest of the Data Subject.

• The transfer is legally required on important public interest grounds.

• The transfer is necessary for the establishment, exercise or defence of legal claims.

• The transfer is necessary in order to protect the vital interests of the Data Subject.

4.10.1 Transfers between Direct Flame Ltd Entities

In order for Direct Flame Ltd to carry out its operations effectively across it's various Direct Flame Ltd Entities, there may be occasions when it is necessary to transfer Personal Data from one Direct Flame Ltd Entity to another, or to allow access to the Personal Data from an overseas location. Should this occur, the Direct Flame Ltd Entity sending the Personal Data remains responsible for ensuring protection for that Personal Data.

Direct Flame Ltd handles the transfer of Personal Data between Direct Flame Ltd Entities, where the location of the recipient Entity is a Third Country, using the Binding Corporate Rules transfer mechanism. Binding Corporate Rules provide legally binding, enforceable rights on Data Subjects with regard to the Processing of their Personal Data and must be enforced by each approved Direct Flame Ltd Entity, including their Employees.

When transferring Personal Data to another Direct Flame Ltd Entity located in a Third Country, you must:

• Ensure that the recipient Direct Flame Ltd Entity is included on the approved list of Direct Flame Ltd Entities subject to the Direct Flame Ltd 'Binding Corporate Rules Agreement'. The approved list is held and maintained by the Office of Data Protection.

• Only transfer the minimum amount of Personal Data necessary for the particular purpose of the transfer (for example, to fulfil a transaction or carry out a particular service).

• Ensure adequate security measures are used to protect the Personal Data during the transfer (including password-protection and Encryption, where necessary).

4.10.2 Transfers to Third Parties

Each Direct Flame Ltd Entity will only transfer Personal Data to, or allow access by, Third Parties when it is assured that the information will be Processed legitimately and protected appropriately by the recipient. Where Third Party Processing takes place, each Direct Flame Ltd Entity will first identify if, under applicable law, the Third Party is considered a Data Controller or a Data Processor of the Personal Data being transferred.

Where the Third Party is deemed to be a Data Controller, the Direct Flame Ltd Entity will enter into, in cooperation with the Office of Data Protection, an appropriate agreement with the Controller to clarify each party's responsibilities in respect to the Personal Data transferred.

Where the Third Party is deemed to be a Data Processor, the Direct Flame Ltd Entity will enter into, in cooperation with the Office of Data Protection, an adequate Processing agreement with the Data Processor. The agreement must require the Data Processor to protect the Personal Data from further disclosure and to only Process Personal Data in compliance with Direct Flame Ltd instructions. In addition, the agreement will require the Data Processor to implement appropriate technical and organisational measures to protect the Personal Data as well as procedures for

providing notification of Personal Data Breaches. Direct Flame Ltd has a 'Standard Data Processing Agreement' document that should be used as a baseline template.

When a Direct Flame Ltd Entity is outsourcing services to a Third Party (including Cloud Computing services), they will identify whether the Third Party will Process Personal Data on its behalf and whether the outsourcing will entail any Third Country transfers of Personal Data. In either case, it will make sure to include, in cooperation with the Office of Data Protection, adequate provisions in the outsourcing agreement for such Processing and Third Country transfers. Direct Flame Ltd has a 'Standard Provisions for outsourcing Agreement' document that should be used for guidance.

The Office of Data Protection shall conduct regular audits of Processing of Personal Data performed by Third Parties, especially in respect of technical and organisational measures they have in place. Any major deficiencies identified will be reported to and monitored by the Direct Flame Ltd Executive Management team.

4.11 Complaints Handling

Data Subjects with a complaint about the Processing of their Personal Data, should put forward the matter in writing to the Office of Data Protection. An investigation of the complaint will be carried out to the extent that is appropriate based on the merits of the specific case. The Office of Data Protection will inform the Data Subject of the progress and the outcome of the complaint within a reasonable period.

If the issue cannot be resolved through consultation between the Data Subject and the Office of Data Protection, then the Data Subject may, at their option, seek redress through mediation, binding arbitration, litigation, or via complaint to the Data Protection Authority within the applicable jurisdiction.

4.12 Breach Reporting

Any individual who suspects that a Personal Data Breach has occurred due to the theft or exposure of Personal Data must immediately notify the Office of Data Protection providing a description of what occurred. Notification of the incident can me made via e-mail servicedesk@directflameltd.com or by calling 02036377951.

The Office of Data Protection will investigate all reported incidents to confirm whether or not a Personal Data Breach has occurred. If a Personal Data Breach is confirmed, the Office of Data Protection will follow the relevant authorised procedure based on the criticality and quantity of the Personal Data involved. For severe Personal Data Breaches, the Direct Flame Ltd Group General Counsel will initiate and chair an emergency response team to coordinate and manage the Personal Data Breach response.

5. Policy Maintenance

All inquiries about this policy, including requests for exceptions or changes should be directed to the Office of Data Protection via e-mail servicedesk@directflameltd.com

5.1 Publication

This policy shall be available to all Direct Flame Ltd Employees in the office.

5.2 Effective Date

This policy is effective as of 25/05/2018 and has been reviewed on 19.06.20 as part of the ISO certificate and document review.

5.3 Revisions

The Office of Data Protection is responsible for the maintenance and accuracy of this policy. Notice of significant revisions shall be provided to Direct Flame Ltd Employees through documentation in the office.

6. Related Documents

Listed below are documents that relate to and are referenced by this policy.

- Internet Privacy Notice template
- Internet Cookie Notice template
- Information Security Policy
- Data Subject Request Handling Procedure
- Data Protection Policy for Employee Data
- Personal Data Retention Schedule
- Standard Data Processing Agreement
- Standard Provisions for Outsourcing Agreement
- Binding Corporate Rules Agreement

Reference	GDPR 01
Version	2.0
Issue Date	19.03.20
Approved	Mark White
Review on	19.09.20

DIRECT FLAME LTD

GDPR POLICY – DATA HANDLING

Appendix A - Information Notification to Data Subjects

The table below outlines the various information elements that must be provided by the Data Controller to the Data Subject depending upon whether or not Consent has not been obtained from the Data Subject.

Information Requiring Notification	With Consent	Without Consent
• The identity and the contact details of the Data Controller and, where applicable, of the Data Controller's representative.	✓	✓
• The original source of the Personal Data, and if applicable, whether it came from a publicly accessible source.	✓	✓
• The contact details of the Data Protection Officer, where applicable.	✓	✓
• The purpose(s) and legal basis for Processing the Personal Data.	✓	✓
• The categories of Personal Data concerned.	✓	✓
• The recipients or categories of recipients of the Personal Data.		✓
• Where the Data Controller intends to further Process the Personal Data for a purpose other than that for which the Personal Data was originally collected, the Data Controller shall provide the Data Subject, prior to that further Processing, with information on that other purpose.	✓	✓
• Where the Data Controller intends to transfer Personal Data to a recipient in a Third Country, notification of that intention and details regarding adequacy decisions taken in relation to the Third Country must be provided.	✓	✓
• The period for which the Personal Data will be stored, or if that is not possible, the criteria used to determine that period.	✓	✓
• Where applicable, the legitimate interests pursued by the Data Controller or by a Third Party.	✓	✓
• The existence of Data Subject rights allowing them to request from the Data Controller- information access, objection to Processing, objection to automated decision-making and profiling, restriction of Processing, data portability, data rectification and data erasure.	✓	
• Where Processing is based on Consent, the existence of the right to withdraw Consent at any time, without affecting the lawfulness of Processing based on Consent before its withdrawal.	✓ ✓	✓
• The right to lodge a complaint with a Data Protection Authority.		✓
• The existence of automated decision-making (including Profiling) along with meaningful information about the logic involved and the significance of any envisaged consequences of such Processing for the Data Subject.	✓	✓
• Whether the provision of Personal Data is a statutory or contractual requirement, a requirement necessary to enter into a contract, as well as whether the Data Subject is obliged to provide the Personal Data and if so the possible consequences of failure to provide such data.		

Appendix B - Adequacy for Personal Data Transfers

The following are a list of countries recognised as having an adequate level of legal protection for the rights and freedoms of Data Subjects in relation to the Processing of their Personal Data.

• EU Countries

(Austria, Belgium, Bulgaria, Croatia, Republic of Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and the UK)

• Iceland

• Liechtenstein

• Norway

• Andorra

• Argentina

• Canada (commercial organisations)

• Faeroe Islands

• Guernsey

• Israel

• Isle of Man

• Jersey

• New Zealand

• Switzerland

• Uruguay

• United States (Privacy Shield certified organisations)

The following are a list of Third Country transfer mechanisms that can provide adequate protection when transfers are made to countries lacking an adequate level of legal protection.

Appendix B - Adequacy for Personal Data Transfers

Appropriate safeguards

• Model Clauses

• Binding Corporate Rules

• Codes of Conduct

• Certification Mechanisms

Derogations

- Explicit Consent
- Compelling Legitimate Interests
- Important reasons of Public Interest
- Transfers in response to a foreign legal requirement
- DPA approved contracts between Data Controllers