A GUIDE* TO THE PRINCIPLES AND BACKGROUND TO GDPR

***This document is provided as guidance and not legal opinion. Should the reader require any further detail it is recommended that they initially look online at the Information Commissioner Office (ICO) website (https://ico.org.uk/) or contact a GDPR expert**

Background to GDPR

Definitions

Consent – Freely given, specific, informed and unambiguous indication of the data subject's wishes by a statement or clear affirmative action
Data Controller – Entity which determines the purpose and means of the processing of personal data
Data Processor - Entity which processes personal data on behalf of the controller
Data Protection Officer – A person who is given formal responsibility for data protection compliance within an organisation
Data Subject – the individual to whom the personal data relates
Direct Marketing – The communication (by whatever means) of any advertising or marketing material which is directed to particular individuals
ICO – Information Commissioner's Office (UK's independent authority responsible for enforcing GDPR)
Personal Data – Any information relating to an identified or identifiable natural person
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
Processing – Any operation performed on personal data ….. such as 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.
Profiling – Any form of automated processing consisting of the use of personal data to evaluate certain personal aspects relating to a natural person (e.g. behaviour, personal preferences, location etc)
Pseudonymous data – The technique of processing personal data in such a way that it can no longer be attributed to a specific data subject**.**
Soft Opt-in – A mechanism by which organisations can market to existing customers on an opt out basis (subject to certain conditions being met)

Key Principles

Comes into effect 25th May 2018

- Fundamental but not an absolute right
- Expectation of lawful processing
- Default 'opt out'
- Appropriate of processing
- Non-jurisdictional legislation

- Definition of personal data - all data which is capable to directly as well as indirectly identify a person, such as online identifiers, location data, IP addresses.
- Obligation to self-report any and all data breaches within 72 hours of becoming aware of it, unless they are unlikely to result in a risk to the rights/freedoms of data subject.
- Clearer definition of certain terms, such as data subject's "consent"
- Stronger rights for data subjects

Data management principles of the GDPR

1. Fair, transparent and lawful processing
2. Purpose limitation
3. Minimization of processing
4. Data Accuracy/Data Quality
5. Retention storage and limitation
6. Security and Confidentiality
7. Liability and accountability

PRINCIPLE 1

1. Fair, **transparent** and **lawful processing** – Personal data shall be processed fairly, lawfully and in a transparent manner in relation to the Data Subject

   Transparency – the following conditions must be set out and made accessible to the data subject in order to constitute as fair and lawful processing of their personal data:

   - The identity of the data controller or any associated third party which will be involved in the processing of the data
   - The purpose for the processing of the data in question
   - Any and all intended recipients or categories of recipients
   - The existence of the right of access to one's own personal data
   - Contact details for the data controller
   - Any other relevant pertinent information which will make the data processing fair for the data subject

Lawful Processing conditions: -

a) The Data Subject has given **consent** to the processing of their personal data for one or more specific purposes
b) The processing is necessary for the **performance of a contract** to which the Data Subject is party in order to take steps at the request of the Data Subject prior to entering into a contract
c) The processing is necessary for the compliance with a in order to protect the **legal obligation** to which the controller is subject
d) The processing is necessary in order to protect the **vital interests** of the Data Subject or of another natural person
e) The 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 controller
f) The processing is necessary for the purposes of the **legitimate interests** pursued by the Controller or by a third party (Processor), except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject which requires protection of personal data, in particular where the data subject is a child.

IN SUMMARY: At least one must apply

a) The **consent** to the processing of personal data for one or more specific purposes is present
b) The processing is necessary for the **performance of a contract**
c) The processing is necessary for compliance with a **legal obligation**
d) The processing is necessary in order to protect **vital interests**
e) The processing is necessary for the performance of a task carried out in the **public interest**
f) The processing is necessary for the purposes of **legitimate interests**, expect where such interests are overridden by the interests of fundamental rights and freedoms of the data Subject which require protection of personal data , in particular where the data subject is a child

CONSENT

Consent must be affirmative

For consent to be valid it should be: -

- Unambiguous
- Freely given
- Specific
- Informed
- An active indication of the subjects wishes
- No pre-ticked boxes

SENSITIVE PERSONAL DATA

The process of the following categories of personal data will be prohibited under GDPR: -

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- The process of genetic data, biometric data in order to uniquely identify a person
- Data concerning the mental or physical health or sex life and sexual orientation of a person

Unless at least one of the following condition applies: -

- The data subject has given **explicit consent** to the processing of those personal data for one or more specified purposes
- The processing is necessary for the purposes of carrying out the obligations of the Controller or of the Data Subject in the field of **employment and social security and social protection**
- The processing is necessary to protect the **vital interests of the Data Subject or of another person** where the Data Subject is physically or legally incapable of giving consent
- The processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other **non-profit seeking body** with a political, philosophical, religious or trade union aim, in connection with its ethos and purposes
- The processing relates to personal data which are **manifestly made public** by the Data Subject
- The processing is necessary for the **establishment, exercise or defense of legal claims** or whenever courts are acting in their judicial capacity
- The processing is necessary for reasons of **substantial public interest**
- The processing is necessary for the purposes of **preventative or occupational medicine**, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services pursuant to contact with a health professional
- The processing is necessary for reasons of public interest in the area of **public health**, such as protecting against serious cross border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices
- The processing is necessary for **archiving purposes in the public interest**, or scientific and historical research purposes in accordance with the Regulation.

Children
Children under the age of 13 can never, themselves give consent to the processing of their personal data in relation to online services.

For children between the ages of 13-15 (inclusive) the general rule is that if an organisation seeks consent to process their personal data then parental consent must be obtained., unless the relevant individual member States legislates to reduce the age threshold – although the threshold can never drop below 13 years of age.

Children aged 16 or older may give consent for the processing of their personal data themselves.

There are no specific rules relating to parental consent for offline data processing; usual Member State rules on capacity would apply here.

The controller is required to make 'reasonable efforts' to verify that consent has been given or authorised by the holder of parental responsibility in light of available responsibility.

IN SUMMARY: At least one must apply

- The Data Subject has given **explicit consent**
- The processing is necessary in the field of **employment and social security and social protection**
- The processing is necessary to protect the **vital interests of the Data Subject or of another person**
- The processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other **non-profit seeking body** with a political, philosophical, religious or trade union aim.
- The processing relates to personal data which are **manifestly made public** by the Data Subject
- The processing is necessary for the **establishment, exercise or defense of legal claims** or whenever courts are The processing is necessary for reasons of public interest in the area of **public health** acting in their judicial capacity
- The processing is necessary for reasons of **substantial public interest**
- The processing is necessary for the purposes of **preventative or occupational medicine**
- The processing is necessary for reasons of public interest in the area of **public health**
- The processing is necessary for **archiving purposes in the public interest**

PRINCIPLE 2

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.

PRINCIPLE 3

3. Minimization of processing – Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

PRINCIPLE 4

4. Data Accuracy/Data Quality – personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay

   The following may be included as obligations required of the Data Controller to ensure that the data that is being processed remains accurate: -

   - Frequency of checks
   - Data quality criteria
   - Completeness
   - Consistency
   - Currency
   - Correct representation of reality
   - Fitness for use
   - Tolerance for inaccuracy

   Key steps to data quality review:

   a) An objective review of the organization's data requirements and quality
   b) Consideration of the organisation's 'appetite' or tolerance for low quality data
   c) Definition of the data quality criteria against which the source data can be evaluated
   d) Conduct a thorough data review to 'weed out' obsolete or unwanted data prior to use
   e) Establishment of appropriate measures and oversight to ensure that these data quality criteria are maintained in the future

PRINCIPLE 5

5. Retention storage and 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 are processed
   - Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research or statistical purposes

Retention considerations

- Rules apply equally to automated and manual data
- If the data needs to be in identifiable format
- Knowing the useful lifespan of the data
- The point of minimum economic value
- Appropriate can cost effective storage
- Business need versus regulatory obligation
- Operational versus historical value
- Proportionate storage solutions
- Efficient retrieval purposes
- Relevant data catalogues
- Appropriate and verifiable destruction

PRINCIPLE 6

6. Security and Confidentiality – taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Controller and the Processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to risk.

   Particular attention should be paid to the following risks:

   - Accidental or unlawful destruction of data
   - Loss of data
   - Accidental or unlawful alteration of data
   - Unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

PRINCIPLE 7

7. Accountability and Liability

   The Data Controller must be able to: –

   - Demonstrate compliance with the requirements of GDPR
   - Place emphasis on proactive methodologies
   - Provide evidence of a 'culture of compliance'
   - Maintain ongoing logs of data breaches
   - Effect the necessary breach notification obligations
   - Provide notification of processing in certain circumstances
     - Controller obligation to maintain log of processing
     - Processor obligation to maintain log of processing
     - Identification of categories of data being processed
     - Identification of categories of processes to be engaged
     - Envisaged time limit for retention

Accountability

- Role of Data Controller - Primary point of compliance
- Role of Data Processor - Mandatory contract in place
- Role of Data Protection Officer - Dedicated role within the organization – Not necessarily an employee
- Individual liability of Board Members.

Data Controller

Data Controller Impact
The GDPR will extend the 'reach' of EU data protection law outside of the EU to non EU companies offering goods or services to residents of the EU or who monitor the behavior of those residents.
Language and focus of GDPR is on the Data Controller being able to demonstrate a 'duty of care' towards the data for which they are responsible.

Processing Activities
In order to demonstrate compliance with the GDPR, each Data Controller and Data Processor will be required to maintain a log or record of processing activities for which it is responsible.

That record should contain all the following information: -

- The name and contact details of the Controller and, where applicable the Joint Controller, the Controller's Representatives and the Data Protection Officer.
- The purposes of the processing
- A description of the categories of Data Subjects and of the categories of personal data
- The categories of recipients to whom the personal data have been or will be disclosed including Recipients in third countries or International organisations
- Where applicable, transfers of personal data to a third country or an international organization including the documentation of appropriate safeguards.
- Where possible, the envisaged time limits for erasure of the different categories of data
- Where possible, a general description of the technical and organisational security measures.

Breach Notification

The Controller is obliged to disclose any incident where the data is exposed to risk, even where the data may not have been disclosed outside the organisation or to an unauthorised individual.

Information should be provided on the following aspects of the incident: -

- A description of nature of the personal data breach
- The categories and approximate number of Data Subjects concerned
- The categories and approximate number of data records concerned
- The name and contact details of the Data Protection Officer or other contact point where more information can be obtained
- A description of the likely consequences of the personal data breach
- A description of the measures taken or proposed to be taken by the Controller to address the personal data breach, including, where appropriate, to mitigate its possible adverse effects

Privacy Impact Assessments

Where processing operations are likely to result in a high risk to the rights and freedoms of natural persons, the Controller will be required to carry out a Privacy Impact Assessment in order to evaluate, in particular, the origin, nature, particularly and severity of that risk.

The following conditions and measures should be taken into account when determining the suitability and practice of a Privacy Impact Assessment.

- Where the personal data processing is likely to give rise to a risk of the data
- Should involve the DPO and other, relevant stakeholders
- Systematic evaluation of proposed processing
- Identification of risk
- Outline of the measures being taken to mitigate those risks
- Outline of structures and measures planned to achieve compliance
- Where substantial risk is identified, the Data Controller must check with the Supervisory Authority.

Overseas Transfer of data

- When personal data is transferred from the EU to Controllers, Processors or other recipients in third countries, the level of protection of individuals should not be undermined
- Transfer to countries outside the EU should take place only where the destination can provide an adequate level of protection for such data
- Binding Corporate Rules
- Model Contracts

Exemptions/Derogations

Circumstances in which the transfer of personal data to a third country, without the adequate safeguards being in place, is permitted.

- Where the data subject has given his or her explicit consent.
- Where the transfer is occasional and necessary in relation to a contract or a legal claim
- Where the transfer is necessary on important grounds of public interest
- Where the transfer is made from a register established by law and intended for consultation by the public.
- Where the transfer is necessary to protect the data subject's or another person's vital interest
- Where the transfer is for scientific or historical research purposes or statistical purposes.

Data Processor Role

- Must be able to provide appropriate technical and organizational structures
- Must be able to demonstrate competence and compliance
- Can only engage sub-contractors with Controller's approval.
- Controller has the right to object to appointment of sub-contractors
- Data Processor contract must be in place, with prescribed clauses
- Same contract clauses and obligations will apply to sub-contractors
- Where Processor determines the processing, they will be treated as a Controller for that proposition of the processing
- Must maintain a written (electronic) log of processing activities
    - Categories of processing
    - Transfer to third countries
    - Detail of Controller on whose behalf the processing is carried out

Data Processor Obligations

- In order for the engagement between the Data Controller and Data Processor to be compliant, a formal, written contract must be in place prior to the processing taking place.

- Since the Data Controller remains the primary entity responsible for the compliance under the Regulation, the Data Controller can determine the parameters and scope of the processing being conducted by the Third party

Data Processing Contract

The contract must set out:
The **subject matter and duration** of the processing
The **nature and purpose** of the processing
The **type** of personal data and **categories** of Data Subjects; and
The **obligations and rights** of the Data Controller

In addition, the contract must provide clauses regarding the following responsibilities of the Processor, including:

- That the Processor only processes the personal data based **on documented instructions** from the Controller;
- That the Processor ensures that persons authorised by the Processor to process the personal data have **committed themselves to protecting the confidentiality** of that data;
- That the Processor takes all appropriate measures required **to ensure the security** of the personal data (with regard to Article 32 of the GDPR);
- That the Processor respects the preferences of the Data Controller with regard to **engaging another processor** or sub-contractor;
- That the Processor assists the Controller by implementing **appropriate technical and organisational measures**, insofar as this is possible, for the fulfilment of the Controller's obligation in responding to requests relating to a data subject's rights;
- That the Processor assists the controller in ensuring compliance with the **obligations regarding data security**, in as far as possible;
- That, at the choice of the Controller, the Processor **deletes or returns all the personal data** to the controller after the end of the provision of services outlined in the contract;
- That the Processor makes available to the controller all information necessary to **demonstrate compliance** with the obligations set out in the Regulation, and allows for and contribute appropriately to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

Management of Subcontractors

Where a processor enlist another Processor for carrying out specific processing activities on behalf of the Controller, it will be the responsibility of the Data Processor to ensure that the same level of protection exists for the data during this element of the processing, as exists between the Data Controller and the data Processor themselves.

Data Processing Liabilities

In a substantial departure from previous Data Protection legislation, the Data Processor will be held liable for any breaches of the Regulation which occur 'downstream' from the Processor i.e. during processing being conducted by a Subcontractor

Data Processor – Logging of Activities

The GDPR stipulates that the Processing Log to be maintained by the Data Processor must contain the following information: -

- The name and contact details of the Data Processor or subcontractor
- The name and contact details of each Data Controller on behalf of which the Processor is acting
- The detail of the controller's or the Processors Nominated Representative
- The details of the Controllers Data Protection Officer, if any
- The categories of processing carried on behalf of each Controller
- Where the processing involves transfers of data to a third country outside the EU, the documentation of appropriate safeguards and, where possible
- A general description of the technical and organisational security measures implemented by the processor

The Data Subject Rights

I. The Right to be Forgotten (Right of Erasure)
II. The Right to Restriction of Processing
III. The Right to Object to Certain Processing
IV. The Right to Data Portability
V. The Right to Access to One's Personal Data
VI. Rights in relation to Profiling and Automated Decision Making
VII. 1 month response time applies to all Data Subject Rights

The Right to be Forgotten
The Data Subject shall have the right to obtain from the Controller the erasure of personal data concerning him or her without undue delay where one of the following grounds applies: -

- The personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed
- The Data Subject withdraws consent
- The Data Subject objects to the processing
- The personal data have been unlawfully processed
- The personal data have to erased from compliance with a legal obligation in Union or Member State law to which the Controller is subject
- The personal data have been collected in relation to the offer of information society services (from children under 16 years of age)

The Right to Restriction of Processing

The Data Subject shall have the right to obtain from the Controller the restriction of the processing of personal data where: -

- The accuracy of the data is contested by the Data Subject, for a period of time, enabling the Controller to verify the accuracy of the data
- The processing is unlawful and the Data Subject opposes the erasure of the data and requests the restriction of their use instead
- The Controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims
- He or she has objected to processing, pending the verification whether the legitimate grounds of the Controller override those of the Data Subject

The Right to Object

- A Data Subject is entitled to object to the processing of their personal data based on his or her particular situation
- The burden is on the Data Controller to be able to demonstrate that the Controller 's compelling legitimate interest overrides the interests of the fundamental rights and freedoms of the data subject
- Otherwise, the Data Subjects objection takes priority

The Right to Data Portability

- The Data Subject should be able to receive a copy of the personal data which he or she has provided to a controller in a structured, commonly used, machine readable and interoperable format.
- The Controller must also be able to transmit this data, at the Data Subject's request, to another controller
- For example, where a Data Subject changes mobile phone services from one provider to another, they can request that their account details, tariff preferences etc, be transferred by the old provider to the new one.

The Right of Access to one's personal data

- Every data Subject should have the right to know: -
- The purposes for which the personal data processed
- The period for which the personal data are processed (where possible)
- The recipients of the personal data
- The logic involved in any automatic personal data processing
- Where profiling is involved, the consequences of such processing

Rights in relation to Profiling and Automated Decision Making

The Data Subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her, unless: -

The processing ….

- Is necessary for entering into, or performance of, a contract between the Data Subject and a Controller

- Is authorised by Union or Member State law to which the Controller is subject and which also lays down suitable measures to safeguard the Data Subject's rights and freedoms and legitimate interests
- Is based on the Data Subject's explicit consent.

The DPO – Profile

- Expertise in the area of EU data protection law
- A good understanding of the way the organisation operates with particular regard to its personal data processing activities
- An ability to interpret relevant data protection rules in that context
- Personal skills including integrity, initiative, organisation, perseverance, discretion, ability to asset himself/herself in difficult circumstances, an interest in data protection and the personal and professional motivation to be a DPO
- Interpersonal skills including communication, negotiation, conflict resolution and the ability to build strong, constructive working relationships
- Have the autonomy, related budget, necessary resources, signing authority and decision-making powers to execute data protection plans and tasks, address non-compliance issues, and report incidents to the relevant Data Protection Supervisory Authority without needing to refer 'up' for authorisation or permission to do so.

The DPO – Role

- To inform and advise the organisation's management and employees who are processing personal data of their obligations under the Regulation
- To keep them advised of their obligations with regard to other data protection provisions
- To monitor the organisation's compliance wit this Regulation and with the policies of the controller or processor in relation to the protection of personal data including: -
    - The assignment of responsibilities
    - Awareness raising
    - Training of staff involved in the processing operations
    - Conducting timely and appropriate audits
- To provide advice where requested as regards the data protection impact assessment and monitor the compliant performance of any solution arsing from a PIA
- To cooperate fully with the respective Supervisory Authority
- To act as the contact point for the Supervisory Authority on issues related to the processing of personal data, including prior consultation with the Supervisory Authority where necessary.

The DPO - Periodic Reporting

- The DPO should prepare a report, normally once or twice a year, to inform his/her organisation, and in particular the senior management team, of the status of the organisation's data protection compliance

- The reports could be published on the organisations intranet site and a copy of these reports should be available to the Supervisory Authority, either by publication or by sending it to the Office Directly.

These reports should include: -

- A status report on notifications, prior checks, and the state of the organisation's risk register
- A summary of any supervision activities of the Supervisory Authority with respect to the organisation the organisation over the relevant period (audits, investigations, guidance, correspondence etc)
- Information on any staff training activities that were provided over the relevant period, and any training planned for the future
- A status report on efforts undertaken to satisfy any recommendations made by the Supervisory Authority in any previous engagements
- Report on requests and complaints received from data subjects, the organisation's responses to date, and their current status
- The results of checks and audits carried out by the DPO in selected parts of the organisation using a rotation system, including conclusions as to the organisation's or department's state of compliance and, where necessary, recommendations to resolve situations of non-compliance.

Exemptions for Specific Data Processing Scenarios

- Freedom of Expression
- Processing of Official Documents
- Processing regarding employment
- Processing for Archiving Purposes
- Processing of Data by Religious Organisations