**Wexford Public Participation Network.**

**Personal Data Protection Policy**

in respect of the General Data Protection Regulation.

REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL.

**"The protection of natural persons in relation to the processing of personal data is a fundamental right"**

Article 8(1) of the Charter of Fundamental Rights of the European Union and Article 16(1) of the Treaty on the Functioning of the European Union provide that everyone has the right to the protection of personal data concerning him or her.

**Context of this Personal Data Protection Policy:**

**This policy must be read in conjunction with the Regulation and Irish Legislation made under it.**

**It sets out how the Wexford Public Participation Network handle and process data, deal with requests for data from a data subject, manage breaches of data and related matters.**

Approved by Wexford PPN Secretariat 12th June 2018.

**Introduction:**

**General Data Protection Regulation.**
The General Data Protection Regulation (GDPR) is in effect from 25th May, 2018 and has repealed the Data Protection Acts 1998 to 2003 and related EU Data Protection Directives.

It is a Regulation and it comes into effect throughout the EU without adoption of legislation by member states except for Articles therein which allow for national interpretation and legalisation.

It consists of 99 Articles which are listed in Appendix 3. However, many of these are not Articles are not directly relevant to County Wexford Public Participation Network.

**Public Participation Networks.**
Public Participation Networks were introduced following the enactment of the Local Government Reform Act 2014. Since then they have been established in each county / city through collaboration between Local Authorities (LAs) and local volunteer / community led organisations.

**Wexford Public Participation Network.**
Wexford Public Participation Network, (hereafter referred to as PPN), was established in 2014 in line with the policy document "Putting People First" pursuant to the above Act.
It operates in line with guidelines issued from the Department of Housing, Planning, Community and Local Government in the publication:

**Public Participation Networks (PPNs) A User Guide, March 2017.**

More recently PPNs' nationally are under the aegis of the Department of Rural and Community Development. The PPN is a collective of environmental, social inclusion, community and voluntary organisations in County Wexford which

- Facilitates the participation and representation of communities in a fair, equitable and transparent manner through the above sectors on decision making bodies
- Strengthens the capacity of these organisations to contribute positively to the community in which they reside / participate
- Provides information relevant to these sectors and acts as a hub around which information is distributed and received.

**PPN Principles and Values:**
The PPN operates under the following principles and values:

- Inclusiveness,
- Participatory,
- Independent of Local Authority and vested interests,
- Valuing Diversity,
- Transparent in its operations and
- Accountable to its member groups.

**Information and Data Gathering.**
The PPN in performing its functions engages with numerous organisations and associations and collects and processes significant amounts of information from these groups. Much of this information is personal data and PPN must adhere to the provisions of the GDPR, any amendments thereto and Irish legislation enacted thereunder. Consent to the use and processing of personal data must be given by

the data subject to PPN who has the right also to withdraw such consent as provided for in Articles 7 and 8.

**Definitions of Personal Data and Consent.**
**'personal data' (Article 4):** means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one 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 to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

**Specific provisions apply to special categories of personal data. (Article 9 applies and must be read in its entirety.)**

**Article 9.1:** "Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.. subject to the provisions of this Article 9……."

**Principles governing data collecting and processing:**
Article 5 of the Regulation provides for the Principles relating to processing of personal data.
Article 6 further governs these principles.
Articles 5 and 6 are set out in Appendix 1.
The principles are summarised as follows:

1. Processing shall be lawful, fair and transparent.
2. Shall be collected for specified, explicit and legitimate purposes.
3. Shall not be further processed in a manner that is incompatible with those purposes. (Exceptions provided for archiving, scientific or historical research or statistical purposes)
4. Shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
5. Accurate and kept up to date; inaccurate personal data is erased or rectified without delay.
6. 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 if it is processed for archiving, scientific or historical research or statistical purposes.)
7. Ensuring security of the personal data, including protection against unauthorised, unlawful processing and against accidental loss, destruction or damage.
8. Consent (defined below) is freely given and lawful processing is adhered to.
9. To be responsible for and be able to demonstrate compliance with the above principles.

**Data Processing and Data Processors:**
In respect of data processing and data processors Articles 7 to 11 apply and it is the policy of PPN to endeavour to comply with these Articles when processing data and engaging with its data processors.
**'consent'** of the data subject means 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;
In collecting and processing personal data the PPN is committed to protecting the rights and privacy of individuals in accordance with the current Regulation and national legislation and with any amendments into the future.

**PPN Commitment on Protection of Personal Data.**
PPN is committed to protecting Personal Data as enshrined in the second title (Freedoms) of the Charter of Fundamental Rights of the European Union which has full legal effect under the Treaty of Lisbon since 1st December 2009 and hereby makes this policy document to underpin same.

**Policy Document.**
This policy document sets out how PPN handles Personal Data within the GDPR. It also references the controls in place in respect of the use of CCTV systems which may come under the control of the PPN and requests for data images from them.

**Data Collection by PPN.**
Data is collected for all of the numerous services the PPN provides to the citizens of County Wexford and from all groups and associations linked to it. It collects data on paper by way of application forms, correspondence etc. It also receives data by way of emails, and online registration and holds data electronically on shared drives and servers.

In all cases it must ensure that data is obtained for stated specified purposes, consent for such data is freely given, that such consent can be withdrawn, that it is held securely and not held for longer than required. Section 2 of the GDPR applies in this respect.

**Definitions.**
Appendix 2 sets out the definitions of the terms used in this policy document as provided for by the GDPR.

**Policies.**
**1. Policy in Respect of Compliance with the General Data Protection Regulation (GDPR).**
It is the policy of PPN to comply fully with the GDPR.
It will, as a Data Control Authority, carry out all duties and functions as set out in the Regulation and related legislation and ensure that the gathering and holding of data is done so solely within the terms of the GDPR.

**2. Policy in respect of Appointment of a Data Controller.**
It is the policy of PPN to have a Data Controller and to adhere to such responsibilities as set out in Articles 24 to 27 inclusive. The PPN Data Controller is the PPN Support Officer as appointed by Wexford PPN Secretariat in adoption of this policy on 12th June 2018. This decision is to be ratified by the Plenary at its next meeting.

**3. Policy in Respect of Register of Data.**
The annual registration of the types and details of data it processes with the Data Protection Commissioners Office is no longer required under the GDPR.
However, in line with good practice the PPN will maintain a register of data as follows:

- A register of all records held by PPN and in which format they are held.
- A description of Personal Data held within these records.
- A list of the persons or bodies to which this Data may be disclosed.
- A list of the Data Processors, Countries or Territories to which the PPN may transfer the Data.
- The uses for which personal data is put.
- Details of the security safeguards in place to protect the privacy of Data held by the PPN.
- The period for which the Personal data will be held.

- Confirmation that consent has been given to the use of the data and the option to withdraw such consent.

**4. Policy in Respect of Adherence with Guidelines issued by the Office of the Data Protection Commissioner.**

It is the policy of the PPN to adhere to all guidelines issued by the Office of the Data Protection Commissioner. These include guidance on such matters as records management, data audits, CCTV guidance as well as rulings in respect of complaints made to that Office.

**5. Policy in Respect of Data Protection Rules.**

It is the policy of the PPN to adhere to the following Data Protection rules and principles which are fundamental to Data Protection law and are contained in the GDPR.
They outline the responsibilities of a Data Controller and its employees in processing personal data. The rules also apply to persons acting as Data Processors on behalf of the Data Controller.

The Rules are:
1. Obtain and process the information fairly.
2. Keep it only for one or more specified, explicit and lawful purposes.
3. Process it only in ways compatible with the purposes for which it was given to the PPN initially.
4. Keep it safe and secure.
5. Keep it accurate and up-to-date.
6. Ensure that it is adequate, relevant and not excessive.
7. Retain it no longer than is necessary for the specified purpose or purposes.
8. Give a copy of his/her personal data to any individual, on request.

**6. Policy in Respect of Rights of the Individual.**

(A Data Subject means an individual who is the subject of personal data, whose rights are set out in Articles 12 to 22 incl.)

**It is the policy of PPN to ensure that the rights of the Individual are fully protected as set out below and the PPN will release information following a request in accordance with these rights:**

Rights of individuals:

1. An individual has the right to find out if the PPN holds data on them.
2. An individual has the right to know the description of any data held on them.
3. An individual has the right to know the purpose for holding such data.
   (Requests for nos. 1 to 3 above must be in writing and is free of charge.)
4. Right of Access. An individual has the right to get a copy of personal information held by a Data Controller about him.
   (This request must be submitted in the form of a written request known as an "Access Request". There is no fee for this information.)
5. An individual has the right of rectification, to be forgotten, erasure and / or blocking if data is no longer relevant or inaccurate.
6. An individual has the right to have their name removed from a direct marketing list such as an edited version of the Electoral Register.
7. An individual has the right to complain to the Data Protection Commissioner if an access request is not responded to fully or partially within set time periods.
8. An individual has the right to seek compensation through the Courts for any harm or distress; e.g., if damage is suffered by an individual through mishandling of data.
9. A Data Subject has the right to withdraw his / her consent to having the data used as originally set out.

**7. Policy in respect of Data Processors.**
It is the policy of PPN to ensure that processors of personal data on its behalf comply fully with the GDPR and Articles 28 to 31 inclusive therein.

**8. Policy in Respect of the Security of Processing by both the Controller and Processor.**
It is the policy of PPN, under Article 32, to ensure the security of personal data in both its operations and those of Data Processors acting on its behalf.

**9.Policy in respect of Managing Data Protection Breaches. (Articles 33 and 34 refer).**
It is the policy of PPN to manage breaches of data protection in accordance with the GDPR, this policy document and guidelines as issued by the Office of the Data Protection Commissioner.

A data protection breach occurs where Personal Data is released without authority or consent.
Such breaches may occur in the event of the loss of USB keys, disks, laptops, digital cameras and mobile phones, or other electronic devices on which data is held, as well as paper records containing data.

A breach may also occur due to inappropriate access to such data on PPN systems or on systems used by Data Processors operating on behalf of PPN including the sending of data to the wrong individuals. In the event of a Data Protection Breach measures will be put in place to prevent a repetition of the incident.

All affected individuals will be notified without delay and an investigation immediately commenced.

The Data Protection Commissioners Office will be contacted, and where the numbers of persons affected exceed a certain limit, all will be notified as directed by that Office.
The findings of the investigation and recommendations will be advised to the Data Protection Commissioners Office and to affected individuals.
All recommendations will be implemented as soon as possible.

**10. Policy in Respect of Promoting Awareness of Data Protection among Staff and others who carry out Data Processing for the PPN.**
It is the policy of the PPN to ensure compliance with the GDPR. It will ensure compliance with the legislation among its staff and groupings and any persons acting as Data Processors on its behalf.
All employees and volunteers of the PPN who collect and / or control the contents and use of personal data are also responsible for compliance with the GDPR.

The PPN will continue to provide support, assistance, advice and Data Protection Awareness training to staff and relevant groupings to ensure compliance with the legislation.

**11. Policy in Respect of a Records Management Policy to ensure the security and ready access of data.**
It is the policy of PPN to implement a Records Management Policy throughout its organisation. These records contain information as well as personal data.

The Policy is designed to facilitate a standardised filing system in which data is securely held and is readily accessible and retrievable in the event of a subject access request and a Freedom of Information request.

In so doing, standardised filing systems, guidance notes on the use of electronic drives, including usage of folder and sub-folder files and categorising and filing of emails will be developed and issued as appropriate.

Personal Data and information can be held on the following:
- Paper records, application forms etc.,
- Electronic Files on Shared and stand-alone drives,
- Emails,
- Diaries,
- Accounts,
- Registers,
- Note Books,
- Tapes,
- DVDs'
- Servers,
- CDs' etc.,
- Website., Intranet.
- Drawings, Maps etc.

The Records Management Policy will also be designed to enable the regular systematic deletion of records in line with the Policy and the rules and principles of the GDPR.
In order to ensure full deletion of the data including all traces of the electronic footprint must be deleted as well as the corresponding paper file.

**12. Policy in Respect of Developing a Data Protection Expertise.**
It is the policy of PPN to train staff in Data Protection law and precedents in order to have that expertise available to advise on queries and subject access requests when received.
The primary point of contact for the public wishing to make subject access requests as well as for contact by the Office of the Data Protection Commissioner is the Support Officer.

**13. Policy in Respect of Handling a Data Subject Access Request. (Article 15).**
It is the policy of PPN to have a central point of access for Data Subject Access Requests as well as providing assistance to requesters. A Data Access Request must meet certain requirements as specified in the GDPR.
These are:

- It must be in writing.
- It must include a reasonable level of appropriate information to enable the PPN to locate the information required.
- PPN will make reasonable enquiries to satisfy itself about the identity of the person making the request to ensure personal data is only released to those entitled to it..
- A 20 day time frame applies to Subject Access Requests. PPN will endeavour to adhere to these. Where reasonable additional information is required to substantiate the request, the time frame for responding runs from receipt of the additional information.
- In the event of receiving a very general Data Access Request, e.g. "please give me everything you have on me", the GDPR provides for the seeking of more detailed information on the nature of the request, such as the approximate date of a particular incident, our reference number, the identity of the other party, etc.

**14. Policy in Respect of an Access Request by others.**
It is the policy of PPN to facilitate requests by the Garda Síochána (or other law enforcement or investigation agency) for access to data from PPN records in relation to the prevention, detection or prosecution of offences or investigations of incidents. The procedure should be that any such request should:

- Be made in writing.
- Provide detail in relation to the data required.
- State the reason it is required.
- Quote the relevant legislation which applies to their request for data.
- Be signed by a person at management level in the organisation, e.g. Garda Sergeant in Charge, Investigating Manager etc.

**15. Policy in Respect of the Further Rights of a Data Subject.**
The PPN will ensure that the rights of the Data Subject as set out in Articles 12 to 22 in respect of such matters as rectification, erasure, right to restriction of processing, data portability etc. will be complied with.

**16. Policy in Respect of Data Controller in relation to Access Requests.**
It is the policy of PPN that the Data Controller will make the final decision as to what should be released and will ensure that the content of data is fully protected, even if released by request.
This role extends to the examination of pixilated CCTV images and stills to ensure no images of persons not making a request are released.

**17. Policy in Respect of Restriction on the Rights of Access(Article 23).**
It is the policy of PPN to examine each subject access request to ensure that data which can be released is released and that restrictions on release under the GDPR and the rights of other data subjects are adhered to.
The release of records and data is governed by the GDPR which also contains some restrictions to the full or partial release of data. These are:
**(**a) national security;
(b) defence;
(c) public security;
(d) the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;
(e) other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation a matters, public health and social security;
(f) the protection of judicial independence and judicial proceedings;
(g) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;
(h) a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points (a) to (e) and (g);
(i) the protection of the data subject or the rights and freedoms of others;
(j) the enforcement of civil law claims.

2. In particular, any legislative measure referred to in paragraph 1 shall contain specific provisions at least, where relevant, as to:
(a) the purposes of the processing or categories of processing;
(b) the categories of personal data;
(c) the scope of the restrictions introduced;
(d) the safeguards to prevent abuse or unlawful access or transfer;
(e) the specification of the controller or categories of controllers;
(f) the storage periods and the applicable safeguards taking into account the nature, scope and purposes of the processing or categories of processing;
(g) the risks to the rights and freedoms of data subjects; and

(h) the right of data subjects to be informed about the restriction, unless that may be prejudicial to the purpose of the restriction.

**18. Policy in Respect of CCTV.**

It is the policy of PPN to develop a policy in respect of CCTV systems, anticipated or otherwise, for any systems operated by it. The policy will distinguish between private and public CCTV and body worn equipment. It will provide for a 28 day deletion of images, restricted access to monitors, servers and recording equipment and security to ensure images are neither deleted or modified.

Requests for images can be made by the Garda Síochána, other enforcement or investigation agencies or the public, who must demonstrate a legitimate reason for a request.

Images released must be pixilated to ensure the privacy of others captured on CCTV.

Applications are made as follows:

- In writing.
- Provide detail in relation to the data required. In particular the time at which an incident
- may have taken place must be specified as extended viewing of captured images is not
- allowed under the GDPR.
- State the reason it is required.
- Quote the relevant legislation which applies to their request for data.
- Be signed by a person at management level in the organisation, as applicable.

**19. Policy in Respect of Data Protection Impact Assessments and Data Protection Officer.**

It is the policy of PPN to adhere to Article 35 and 36 to assess new technologies of data processing to establish the impact on the protection of personal data and to consult with the Office of the Data Commissioner where a high risk may occur.

The PPN, as Data Controller, will examine the provisions of Article 37 in respect of the appointment of a Data Protection Officer (DPO) and notes the position which the DPO may hold within the organisation as well as the DPO's tasks as set out in Article 39.

**20. Policy in Respect of Transfer of Personal Data to Third Countries and International Organisations.**

It is the policy of PPN to adhere to Articles 44 to 50 incl. and to ensure that Data Processors acting on its behalf adhere to these Articles in cases where personal data may be transferred to third countries or international organisations.

**21. Policy in respect of the Review of this Policy Document and New EU Data Protection Regulations and Directives as well as national legislation.**

It is the policy of PPN to review this policy periodically in light of its operation and in terms of new legislative or other relevant factors and following guidance from the Office of the Data Protection Commissioner.

---

Approved by Wexford PPN Secretariat 12th June 2018.

**Appendix 1. Principles relating to processing of personal data.**

CHAPTER II: Principles: Article 5

1. Personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

(d) 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 ('accuracy');

(e) 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 purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');

(f) 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 ('integrity and confidentiality').

2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

Article 6: Lawfulness of processing

1. Processing shall be lawful only if and to the extent that at least one of the following applies:

(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

(b) 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;

(c) processing is necessary for compliance with a legal obligation to which the controller is subject;

(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

(e) 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) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

(Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.)

**Appendix 2. Definitions:**

Article 4 of the GDPR contains all the GDPR definitions. The main ones affecting PPN are as follows:

**'personal data'** means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one 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 to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

**'processing'** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, 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;

**'restriction of processing'** means the marking of stored personal data with the aim of limiting their processing in the future;

**'profiling'** means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

**'pseudonymisation'** means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

**'filing system'** means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;

**'controller'** means the 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; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

**'processor'** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

**'recipient'** means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;

**'third party'** means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;

**'consent'** of the data subject means 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;

**'personal data breach'** means 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;

**'genetic data'** means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;

**'biometric data'** means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;

**'data concerning health'**
means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;

**'main establishment'** means:
(a) as regards a controller with establishments in more than one Member State, the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment;
(b) as regards a processor with establishments in more than one Member State, the place of its central administration in the Union, or, if the processor has no central administration in the Union, the establishment of the processor in the Union where the main processing activities in the context of the activities of an establishment of the processor take place to the extent that the processor is subject to specific obligations under this Regulation;

**'representative'** means a natural or legal person established in the Union who, designated by the controller or processor in writing pursuant to Article 27, represents the controller or processor with regard to their respective obligations under this Regulation;

**'enterprise'** means a natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity;

**'group of undertakings'** means a controlling undertaking and its controlled undertakings;

**'binding corporate rules'** means personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity;

**'supervisory authority'** means an independent public authority which is established by a Member State pursuant to Article 51;

**'supervisory authority concerned'** means a supervisory authority which is concerned by the processing of personal data because:

(a) The controller or processor is established on the territory of the Member State of that supervisory authority;
(b) data subjects residing in the Member State of that supervisory authority are substantially affected or likely to be substantially affected by the processing; or
(c) complaint has been lodged with that supervisory authority;

**'cross-border processing'** means either:

(a) processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or
(b) processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State.

**'relevant and reasoned objection'** means an objection to a draft decision as to whether there is an infringement of this Regulation, or whether envisaged action in relation to the controller or processor complies with this Regulation, which clearly demonstrates the significance of the risks posed by the draft decision as regards the fundamental rights and freedoms of data subjects and, where applicable, the free flow of personal data within the Union;

**'information society service'** means a service as defined in point (b) of Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council;

**'international organisation'** means an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries.

**Appendix 3. The General Data Protection Regulation summary.**

REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

The GDPR will come into effect on 25th May, 2018.

The main provisions are as follows:
Article 1: Subject-matter and objectives
Article 2: Material Scope
Article 3: territorial Scope
Article 4: Definitions.
Article5: Principles relating to the processing of data
Article 6: Lawfulness of processing
Article7: Conditions for consent
Article 8: Conditions applicable to child's consent in relation to information society services
Article 9: Processing of special categories of personal data
Article 10: Processing of personal data relating to criminal convictions and offences
Article 11: Processing which does not require identification.
Article 12: Transparent information, communication and modalities for the exercise of the rights of the data subject
Article 13: Information to be provided where personal data are collected from the data subject
Article 14: Information to be provided where personal data have not been obtained from the data subject
Article 15: Right of access by the data subject
Article 16: Right to rectification
Article 17: Right to erasure ('right to be forgotten')
Article 18: Right to restriction of processing
Article 19: Notification obligation regarding rectification or erasure of personal data or restriction of processing
Article 20: Right to data portability
Article 21: Right to object
Article 22: Automated individual decision-making, including profiling
Article 23: Restrictions
Article 24: Responsibility of the controller
Article 25: Data protection by design and by default
Article 26: Joint controllers
Article 27: Representatives of controllers or processors not established in the Union
Article 28: Processor
Article 29: Processing under the authority of the controller or processor
Article 30: Records of processing activities
Article 31: Cooperation with the supervisory authority
Article 32: Security of processing
Article 33: Notification of a personal data breach to the supervisory authority
Article 34: Communication of a personal data breach to the data subject
Article 35: Data protection impact assessment
Article 36: Prior consultation
Article 37: Designation of the data protection officer
Article 38: Position of the data protection officer
Article 39: Tasks of the data protection officer

Article 40: Codes of conduct
Article 41: Monitoring of approved codes of conduct
Article 42: Certification
Article 43: Certification bodies
Article 44: General principle for transfers
Article 45: Transfers on the basis of an adequacy decision
Article 46: Transfers subject to appropriate safeguards
Article 47: Binding corporate rules
Article 48: Transfers or disclosures not authorised by Union law
Article 49: Derogations for specific situations
Article 50: International cooperation for the protection of personal data
Article 51: Supervisory authority
Article 52: Independence
Article 53: General conditions for the members of the supervisory authority
Article 54: Rules on the establishment of the supervisory authority
Article 55: Competence
Article 56: Competence of the lead supervisory authority
Article 57: Tasks
Article 58: Powers
Article 59: Activity reports
Article 60: Cooperation between the lead supervisory authority and the other supervisory authorities concerned
Article 61: Mutual assistance
Article 62: Joint operations of supervisory authorities
Article 63: Consistency mechanism
Article 64: Opinion of the Board
Article 65: Dispute resolution by the Board
Article 66: Urgency procedure
Article 67: Exchange of information
Article 68: European Data Protection Board
Article 69: Independence
Article 70: Tasks of the Board
Article 71: Reports
Article 72: Procedure
Article 73: Chair
Article 74: Tasks of the Chair
Article 75: Secretariat
Article 76: Confidentiality
Article 77: Right to lodge a complaint with a supervisory authority
Article 78: Right to an effective judicial remedy against a supervisory authority
Article 79: Right to an effective judicial remedy against a controller or processor
Article 80: Representation of data subjects
Article 81: Suspension of proceedings
Article 82: Right to compensation and liability
Article 83: General conditions for imposing administrative fines
Article 84: Penalties
Article 85: Processing and freedom of expression and information
Article 86: Processing and public access to official documents
Article 87: Processing of the national identification number
Article 88: Processing in the context of employment

Article 89: Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes
Article 90: Obligations of secrecy
Article 91: Existing data protection rules of churches and religious associations
Article 92: Exercise of the delegation
Article 93: Committee procedure
Article 94: Repeal of Directive 95/46/EC
Article 95: Relationship with Directive 2002/58/EC
Article 96: Relationship with previously concluded Agreements
Article 97: Commission reports
Article 98: Review of other Union legal acts on data protection
Article 99: Entry into force and application.

ends.