DATA ESSENTIALS
CLIENT GUIDANCE WORKBOOK

Confidence, Assurance and Certainty

CERTIFICATION EUROPE™

INTRODUCTION

What is GDPR?

The EU General Data Protection Regulation is a risk-based regulation, with an objective to enhance and standardise the approach for the protection of personal data. The GDPR will come into effect on 25th May 2018, replacing the various existing Data Protection Acts present in EU member countries. It will affect all organisations involved in processing the data of EU citizens, whether they are operating in an EU member state or not.

What does it mean to me?

It means that organisations will need to carefully consider the data they process and how they can be compliant with the GDPR and its 6 principles. Compliance with current data protection law is not completely sufficient, as the requirements of the GDPR are new and enhanced, to reflect the growing importance and rapid progression of data processing in recent times.

Non-compliance with the GDPR will be met with hefty financial penalties – in the case of a serious infringement a penalty of up to €20,000,000 or 4% of annual global turnover, depending on whichever is greater, could be applied. A company can also be fined 2% of annual global turnover or €10 million for not having their records in order or failing to notify the supervising authority and data subject about a breach

THE APPLICATION PROCESS

All of the question on the following pages are included in the online questionnaire at www.dataessentials.ie

Once you feel you can answer all of the questions you can begin your online application. You can save drafts and return to your application at a later date as well.

Many of the questions have multiple choice answers such as Yes, No, Don't Know. Answering any of these questions No or Don't Know will result in the assessor failing you on that question and requiring further feedback from you.

All of the questions are designed to check if the core requirements of GDPR are being met. If you don't have some of the requirements in place, you should begin implementing these requirements prior to GDPR coming into place.

Once you complete the application one of our assessors will review your application and return a report detailing what areas you need to work on to meet the requirements of GDPR.

If you have successfully met all of the requirements you will receive a certificate of attestation stating that based on answers provided you have all of the core policies, procedures and processes in place to meet GDPR requirements.

GOVERNANCE FRAMEWORK

To support accountability requirements and to demonstrate preparedness.

#	Questions	Answer	Suggestions and Guidance
1	Are the following relevant stakeholders aware of the law and of their obligations under it? 1. Senior management 2. Executive staff 3. Suppliers and other contractors 4. Other Personnel		Please state that all relevant stakeholders are aware of their obligations and refer to how this was achieved.
2	Are you: 1. A Data Controller 2. A Data Processor 3. A Joint Controller or both 4. More than one of the above		Describe your responsiblities under GDPR by selecting one of the listed roles or by describing your particular role, for example; We are a sub processor of personal data for a data controller/processor.
3	If you are more than one of the above, have you identified the data categories in respect of which you hold for each role?		State the identified data categories for your role(s).
4	Have you determined: 1. The categories of personal data that you hold		Reply to each question to the best of your ability and in numerical order, i.e.

#	Questions	Answer	Suggestions and Guidance
	2. The categories of data subjects 3. The purpose for which you hold each category of data 4. The processing to which each category is subject, with data flows mapped out 5. The legal basis on which you are processing each category 6. The categories of recipients of personal data 7. All transfers of data to a non-EEA country 8. Time limits for retention of each category of personal data 9. Any instances within your organisation of Automated Decision-making		1. List of categories 2. List categories of Data Subjects 3. Etc. 4. Etc.
5	Regarding question C and D have you: 1. compiled the information into a record of processing activity 2. two separate records of processing activity where you are both data controller and processor 3. a documented process in place for keeping the Record up to date		Describe the recording proceedures i.e we have completed a data mapping exercise and have compiled a data register/ inventory.
6	Have you developed a: 1. Data Protection Policy 2. Data Security Policy 3. Data Retention & Deletion Policy		Give details of any developed policy or policies that would meet requirements. For example we have an Information Security Pollicy which details all data security requirements.

#	Questions	Answer	Suggestions and Guidance
	4. Data Management Policy 5. None of the above		
7	Do you have: 1. a defined process for determining when a Data Protection Impact Assessment should be carried out 2. a defined process for the performance of Data Protection Impact Assessments 3. Records of all Data Protection Impact Assessments already carried out within the organisation		Describe the process or methodology or supply relevant PIA documentation as evidence (completed PIA etc.). The PIA coud be part of an existing Risk Framework.
8	Have you established an awareness campaign within the organisation dealing with 1. The actions necessary to prepare for GDPR Ongoing Data Protection awareness		Give details of any awareness campaigns already completed and those activities for ongoing awreness that have been planned or scheduled.
9	Do you have an Incident Management process (including a testing process) to deal with Data Breaches, and have all staff and processors been made aware of it?		Describe the process or refer to relevant process documentation, testing plans or schedules. Records of completed tests should also be supplied or described.
10	Have you identified all third parties who may be processors, sub-processors or joint controllers?		Describe how this was completed and reference any supporting documentation.

#	Questions	Answer	Suggestions and Guidance
11	Have all processor contracts been reviewed to ensure that they are sufficient to meet GDPR requirements?		Describe how this was completed and reference any supporting documentation.
12	Have you: 1. identified all processes involving the transfer of data, either by you or a processors to countries outside the EEA 2. ensured that your processors identified all sub-processors who may transfer data to countries outside the EEA 3. the correct legal arrangements in place to transfer personal data to 3rd countries 4. ascertained that your processors or their sub-processors have the correct legal arrangements in place to transfer personal data to 3rd countries		Supply answers with a summary of compliance for each relevant question and in numerical order. *A robust Supplier Relationship/ Management Process could be referenced.*

1 LAWFUL, FAIR AND TRANSPARENT PROCESSING

Principle 1. Lawful, fair and transparent processing is about emphasizing transparency for data subjects.

#	Questions	Answer	Suggestions and Guidance
1.1	Have you determined and documented the lawful basis upon which you are collecting and processing each category of personal data?		Desribe how this was determined and reference the specific documentation or record(s).
1.2	Where consent is the basis on which processing occurs, have you implemented a data subject consent process in place that demonstrably ensures that: 1. Consent has been freely given 2. Consent is specific to the purpose 3. Data subject can withdraw consent as easily as give it 4. Consent for processing of special categories of personal data is explicit 5. A child consent process is in place		Describe the data subject consent process and answer each question in numerical order.
1.3	Do your data collection processes adequately notify data subjects of: 1. the identity and the contact details of the controller or its representative;		Describe how you achieve the requirement to notify and answer each question in numerical order.

#	Questions	Answer	Suggestions and Guidance
	2. the contact details of the data protection officer 3. the purposes of the processing 4. details of the legitimate interest the processing is based on 5. the recipients or categories of recipients of the personal data 6. the retention periods in place 7. details of third country transfers 8. the existence of the rights specified under GDPR 9. None of the above		

2 PURPOSE LIMITATION

Principle 2. Purpose limitation requires having a lawful and legitimate purpose for processing the information in the first place.

#	Questions	Answer	Suggestions and Guidance
2.1	Have you identified and documented the specific purpose for each personal data processing activity?		Describe how this was completed and reference any supporting documentation.
2.2	Does the purpose ensure that personal data is collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes?		Describe how this was completed and reference any supporting documentation (if applicable).
2.3	Do you have measures in place to restrict processing beyond this specific purpose?		Reference any pupose limitation restriction measures.

3 DATA MINIMISATION

Principle 3. Data minimisation is making sure that data is adequate, relevant & limited and organisations are sufficiently capturing the minimum amount of data needed to fulfill the specified purpose.

#	Questions	Answer	Suggestions and Guidance
2.1	Is all personal data collected and processed adequate, relevant and limited to the minimum necessary required for the specific purpose?		Explain how this requirement is realised.
2.2	Where data has been identified which goes beyond what is relevant and necessary for the purpose, do you have processes in place to erase or otherwise cease processing it?		Refer to any appropriate processes to ensure that data that is not relevant is managed (identified, reviewed and erased or otherwise securely removed, delieted or destroyed)

4 DATA ACCURACY

Principle 4. Requires accurate and up-to-date processing where data controllers have to make sure that information remains accurate, valid and fit for purpose.

#	Questions	Answer	Suggestions and Guidance
4.1	Do you have measures in place to ensure that data is accurate and up to date?		Refer to any data review or data management processes
4.2	Do you have measures in place to rectify or erase inaccurate data without delay?		Refer to any manual or automatted measures used to ensure that you can modify erroneous data and describe the time required to do so (or refer to tests).

5 STORAGE LIMITATION

Principle 5. Limitation of storage of data in a form that permits identification thereby discouraging unnecessary data redundancy and replication.

#	Questions	Answer	Suggestions and Guidance
5.1	Do you have a documented data retention policy with an appropriate retention schedule which permits identification of data subjects for no longer than is necessary?		Refer to the data retention policy or procedures used to maintain data for the specified limit.
5.2	Does the Retention Policy provide for regular purging of documents held in contravention of the periods set out in the policy?		Refer to the data retention policy or procedures used to maintain data for the specified limit.

6 INTEGRITY AND CONFIDENTIALITY

Principle 6. Protecting the integrity and privacy of data by making sure that it's secure (which extends to IT systems, paper records or other none IT media and physical security).

#	Questions	Answer	Suggestions and Guidance
6.1	Have you adopted any accredited certification schemes such as: ISO 27001, Cyber Essentials or PCI DSS in order to help demonstrate compliance?		Any certificates must be valid and copies will need to be supplied as evidence. Certification expiry dates must also be described.
6.2	Have you sufficient physical and logical controls in place to protect data from loss, destruction, falsification, unauthorised access and release? Controls must include consideration of: 1. Firewalls or network perimeter controls 2. Secure configuration 3. User access control 4. Malware protection 5. Patch management 6. Physical and environmental		Describe the controls in place or reference how existing certifications meet requirements i.e. *We are certified to ISO 27001 which ensures that we maintain relevant controls.*
6.3	Do you use anonymisation or pseudonymisation for protecting identity?		Descrive how this is achieved and/or reference any cryptographic controls, encryption techniques or other relevant processes.

#	Questions	Answer	Suggestions and Guidance
6.4	Are your anonymisation or pseudonymation techniques sufficient to ensure that the identity of the data subject cannot be determined?		Descrive how this is achieved and/or reference any cryptographic controls, encryption techniques or other relvent processes.
6.5	Do you use encryption to protect data in accordance with the risk and have a relevant encryption policy?		Descrive how this is achieved and reference any cryptographic controls, encryption techniques or other relvent processes.
6.6	Do you have an established and tested data breach or incident management process that is ready and capable to respond to any breach of security swiftly & effectively within 72 hours of discovery?		See Governance Question (J) (incorrect reference and describe how the process is capable of responding to any breach within the required timeframe.
6.7	Do you have disaster recovery or continuity procedures?		Reference any Business Continuity (BCM), Redundancies and disaster recovery (DR) plans including backup and restoration procedures, if applicable.

7 ACCOUNTABILITY

The Accountability Prinicple is a General principle which requires that any organisation must have an appropriate framework to ensure and demonstrate compliance. It is the combination and culmination of all of the 6 principles listed above and the governance structures and mechanisms.

#	Questions	Answer	Suggestions and Guidance
7.1	Do you have documented organisational and technical measures to ensure compliance, including: 1. Data protection policy 2. Data security policy 3. Data Retention policy 4. Staff awareness and training 5. Adequate employment contracts 6. Internal audits of processing activities 7. Reviews of internal HR policies 8. Relevant documentation on processing activities 9. Record of Processing Activities		Refer to all relevant documentation and records or appropriate procedures and reply to each question in numerical order. (If already referenced above please state where it is referenced and move on to next question)
7.2	Have you appointed a data protection officer?		Describe the role and responsibilities and reference organisational position and reporting function or if it is outsourced, list details of supplier/ contractor etc.
7.3	Regarding the Data Protection Officer (DPO):		Describe how the role of DPO or competent personnel has been defined and assigned

#	Questions	Answer	Suggestions and Guidance
	1. Do you have a DPO 2. Have role and responsibilities of the DPO's been defined 3. is your DPO adequately qualified 4. Does your DPO report to the highest level of management within the company		List role and responsibilities, relevant qualifications and place in organisational hierarchy(if applicable) or reporting structure.
7.4	If you have not appointed a data protection officer, do you have documentation to support your decision not to appoint one?		Refer to decision making process and reference supporting documentation or records etc.
7.5	Do your policies embody and ensure the principles of data protection by design and data protection by default? Measures should include: (not fully clear on this on) 1. Data minimisation 2. Pseudonymisation 3. Transparency 4. Allowing individuals to monitor processing 5. Creating and improving security features on an ongoing basis. 6. Using Privacy impact assessments		Review all of the answers given throughout the questionnaire and refer to either the relevant answer/section and specify how the policies ensure data protection by design and reference if they include the measures mentioned in the question.

CLIENT NOTES

CLIENT NOTES