ASMGi
I.T. when security matters

General Data Protection Regulation (GDPR) READINESS ASSESSMENT

The General Data Protection Regulation (GDPR) has been designed to enable individuals to better control their personal data. It is also believed that these rules will make it simpler and cheaper for organizations to do business across the European Union. The GDPR requires organizations to demonstrate compliance with the data protection principles and take a risk-based approach to data protection. The GDPR goals are to ensure appropriate policies and procedures are in place to deal with the transparency, accountability and individuals' rights, as well as build a workplace culture of data privacy and security.

The General Data Protection Regulation (GDPR) not only applies to businesses in the EU, but to all businesses marketing services or goods to EU citizens, regardless of its location. GDPR requirements apply to each member state of the European Union, aiming to create more consistent protection of consumer and personal data across EU nations. Some of the key privacy and data protection requirements of the GDPR include:

- *Requiring the consent of subjects for data processing*
- *Anonymizing collected data to protect privacy*
- *Providing data breach notifications*
- *Safely handling the transfer of data across borders*
- *Requiring certain companies to appoint a data protection officer to oversee GDPR compliance*

The purpose of the GDPR is to impose a uniform data security law on all EU members, so that each member state no longer needs to write its own data protection laws and laws are consistent across the entire EU. As a result, GDPR will have an impact on data protection requirements globally. Any company that stores or processes personal information about EU citizens within EU states must comply with the GDPR, even if they do not have a business presence within the EU. Specific criteria for companies required to comply are:

- *A presence in an EU country*
- *No presence in the EU, but it processes personal data of European residents*

GDPR READINESS CHECKLIST

The table below can be used to determine your companies readiness for GDPR compliance.

	BACKGROUND	QUESTION	
ORGANIZATIONAL STRUCTURE	*Supervisory Authorities have broad powers over the activities of data collectors.*	Can your organization provide Supervisory Authorities the information they require for the performance of their tasks?	☐
	Data Protection Officer	Does your organization have a named Data Protection Officer (DPO)?	☐
DATA BREACH	*Communication of a data breach. Your organization must notify the appropriate supervisory authorities within 72 hours after becoming aware of it where feasible.*	Does your organization's data breach policy and notification process meet GDPR requirements?	☐
DATA COLLECTION	*Your organization must be able to prove that they have successfully collected the data subjects' consent to process their data according to Article 7 and Article 30.*	Can your organization prove they have met GDPR requirements for data collection, including when consent was given, who gave consent and the purpose for which the data was collected?	☐
	Parental Consent	Does your organization make reasonable efforts to verify that they are not collecting any personal information from a child who is below an age where parental co-consent is required?	☐
DATA PROTECTION	*Data Protection and Privacy by Design*	Does your organization have a Written Information Security Plan (WISP) that documents the technologies, products, processes, procedures, plans, policies, mechanisms and organizational structures that are used to protect key business assets?	☐
	Testing Data Protection Measures	Does your organization perform testing of its security measures, whether through technical means, assessments or tabletop exercises?	☐
DATA USE	*Data Privacy and Storage*	Can the organization generally identify all locations where personal data is stored across the enterprise, including on internal servers or cloud storage, as well as those hosted by any third-party providers?	☐

	BACKGROUND	QUESTION	
DATA USE	*Data Inventory*	Does the organization have a tool to catalog how and where personal data is used, and is it partially or fully populated?	☐
	Data Governance Program	Does the organization have a data governance program?	☐
	Data Use by Automated Means	Can your organization identify decisions (e.g. credit checks, background checks) for data subjects that are performed completely or partially by automated means?	☐
	Individuals have the right to transmit their data to another controller without hindrance from the controller to which the data have been provided.	Does your organization provide individuals the capability to transmit their data to another controller?	☐
	Right to be Forgotten	Does your organization provide individuals the capability to easily obtain the erasure of personal data concerning him or her without undue delay from your organizational systems?	☐
	Data Flows Through the EU	Does your organization have documentation of ongoing personal data transfers into and out of the EU?	☐
MANAGING CONSENT	*Individuals shall have the right to obtain from your organization confirmation as to if personal data concerning him or her are being processed, where that data is being processed and who has access to it.*	Does your organization provide individuals the capability to manage consent for who access their data and for what purpose their data is accessed?	☐
PRIVACY NOTICE	*GDPR law says that this privacy notice should be "explicit," "specific," "informed," and "intelligible." It should be "easily accessible" and use "clear and plain language" to convey all the information required by the law in a form that holds the data subject's interest and allows them to digest the notice.*	Does your organization display a privacy notice before collecting personal data?	☐
	Your privacy notice must contain certain language regarding requesting consent for personal data storage and use.	Does your organization privacy notice contain the language that complies with GDPR requirements?	☐

	BACKGROUND	QUESTION	
PRIVACY NOTICE	*Your privacy notice must contain certain language regarding requesting consent for personal data storage and use.*	**Does your organization privacy notice contain the language that complies with GDPR requirements?**	☐
RISK MGMT	*Risk Management Strategy and Program*	**Does your organization maintain a formal risk management program that includes considerations for data privacy?**	☐
THIRD PARTY DATA USE	*Third-Party/Vendor Assessment*	**Does your organization maintain an inventory of vendors/suppliers/third-party services providers that processes and/or store personal data?**	☐
	Third-Party/Vendor Assessment	**Does your organization ensure that your vendors, partners and third-party service providers will NOT use the data collected for any other purpose except those mandated by your organization?**	

Need a more thorough assessment? Or help remediating?
Contact us at 216-255-3045 or asmgi.com

APPENDIX A – Supervisory Authority

For many organizations, identifying their lead supervisory authority (LSA), the principal EU regulator responsible for enforcement of the GDPR in relation to cross border processing, will be straightforward. For others, with data decision-makers in various parts of the EU or with decision-making power regarding data taken outside of the EU but processing data affecting individuals in multiple Member States, it will not be. The LSA is the data regulator in the country in which the controller or processor has its "main establishment" for data processing purposes.

Under the GDPR the "main establishment" of a controller:

- *is the place of its "central administration" in the EU unless*
- *the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the EU that has the power to have such decisions implemented, in which case that is location of the main establishment.*

The GDPR is not a perfect instrument. It does not properly address how an entity with its central administration outside of the EU should determine its LSA. This is acknowledged to be an issue already by the Article 29 Working Party, which noted that there will be "borderline and complex situations where it is difficult to identify the main establishment or to determine where decisions about data processing are taken." Please refer to Article 29 in determining the location of a controller's "main establishment" in cases where central administration is not in the EU.

Given that breaches of the GDPR could result in fines of up to 4% of a company's global turnover, or €20 million, whichever is the greater, organizations will generally want to deal with a regulator in a jurisdiction with a language, legal system and business environment with which they feel comfortable. For many English-speaking organizations with headquarters outside of the EU, Ireland will be an obvious location to consider when planning for enforcement, as it will be the only English speaking, common law Member State post-Brexit.

APPENDIX B – DPO

A Data Protection Officer has formal responsibility for data protection compliance within an organization. The appointment of a DPO under the EU General Data Protection Regulation (GDPR) is only mandatory in three situations:

When the organization is a public authority or body, or when the organization's core activities consist of either:

A. Data processing operations that require regular and systematic monitoring of data subjects on a large scale; or

B. Large-scale processing of special categories of data (i.e. sensitive data such as health, religion, race, sexual orientation, etc.) and personal data relating to criminal convictions and offences.

There is no exemption for small and medium-sized enterprises (SMEs), which has been reaffirmed by the Information Commissioner's Office (ICO). Data protection laws in Germany, for example, require every

APPENDIX B – DPO

business with ten or more employees that permanently process personal data to appoint a DPO. Even where the GDPR does not specifically require the appointment of a DPO, it is highly encouraged by the European Article 29 Working Party (WP29) as a matter of good practice and to demonstrate compliance. It is important to note that an organization that appoints a DPO voluntarily must still comply with the full range of DPO requirements in the GDPR.

The GDPR is explicit about the tasks that DPOs are required to perform. They include the following:

1. Inform and advise the organization and its employees of their data protection obligations under the GDPR.

2. Monitor the organization's compliance with the GDPR and internal data protection policies and procedures. This will include monitoring the assignment of responsibilities, awareness training, and training of staff involved in processing operations and related audits.

3. Advise on the necessity of data protection impact assessments (DPIAs), the manner of their implementation and outcomes.

4. Serve as the contact point to the data protection authorities for all data protection issues, including data breach reporting.

5. Serve as the contact point for individuals (data subjects) on privacy matters, including subject access requests.

The GDPR does not specify the precise credentials a DPO is expected to have. However, in its recent published guidelines the WP29 defines certain minimum requirements regarding the DPO's expertise and skills. The regulation states:

1. Level of expertise – understanding how to build, implement and manage data protection programs is essential. The more complex or high-risk the data processing activities are, the greater the expertise the DPO will need.

2. Professional qualities – DPOs do not have to be lawyers, but they must have expertise in national and European data protection law, including an in-depth knowledge of the GDPR. DPOs must also have a reasonable understanding of the organization's technical and organizational structure and be familiar with information technologies and data security.

The GDPR requires that the DPO operates independently and without instruction from their employer over the way they carry out their tasks. This includes instructing the DPO on "what result should be achieved, how to investigate a complaint or whether to consult the regulatory authority". Nor can organizations tell their DPO how to interpret data protection law.

Although the GDPR allows DPOs to "fulfil other tasks and duties", organizations are obliged to ensure that there is no "conflict of interests" between those activities and the formal duties prescribed under the Regulation. Most senior positions within an organization are likely to conflict with the DPO's duties (e.g. chief executive, chief operating officer, chief financial officer, chief medical officer, head of marketing, head of HR or head of IT).

The DPO cannot be dismissed or penalized for performing their tasks, and organizations must ensure that the DPO reports directly to "the highest management level" in the organization.

The task of the DPO to monitor the organization's compliance with the GDPR does not make the DPO individually liable for non-compliance by the organization. The WP29 states that organizations are

APPENDIX B – DPO CONTINUED

free to ignore the advice of DPOs as they remain "responsible for compliance", but when doing so must document in writing the reasons for not following the advice.
Businesses should assess whether they are obliged to appoint a DPO under the new Regulation, and consider the requirements that DPOs act independently and without conflict when performing their formal tasks.

The GDPR allows organizations to choose whether to appoint an internal or external DPO. Whatever the decision, IT Governance can help your organization fulfil the DPO role.

APPENDIX C – WISP

A Written Information Security Program (WISP) documents the measures that a business, or Organization takes to protect the security, confidentiality, integrity, and availability of the personal information and other sensitive information it collects, creates, uses, and maintains.

The objective of a WISP is to is to create effective administrative, technical and physical safeguards for the protection of personal and regulated information held by an organization. The WISP sets forth procedures for evaluating an organization's electronic and physical methods of accessing, collecting, storing, using, transmitting, and protecting personal and regulated information.

The WISP typically serves as a foundational element in an organization's information security program. It often stands alone and documents the scope, purpose, risk management, mechanisms, elements, policies, procedures, processes, programs and documents used to establish, operate and measure an information security program.

APPENDIX D – DATA GOVERNANCE PROGRAM

Data governance (DG) is the overall management of the availability, usability, integrity and security of data used in an enterprise. A sound data governance program includes a governing body or council, a defined set of procedures and a plan to execute those procedures.

Businesses benefit from data governance because it ensures data is consistent and trustworthy. This is critical as more organizations rely on data to make business decisions, optimize operations, create new products and services, and improve profitability.

APPENDIX E – DATA CONTROLLER / DATA PROCESSOR

The Data Controller is the entity that determines the purposes, conditions and means of the processing of personal data.

The Data Processor is the entity that processes data on behalf of the Data Controller.

APPENDIX E – DATA CONTROLLER / DATA PROCESSOR CONTINUED

The GDPR places specific legal obligations on a Processor. Processors are required to maintain records of personal data and processing activities. Processors have legal liability if they are responsible for a breach.

Controllers are not relieved of your GDPR obligations. Controllers must ensure their contracts with Processors comply with the GDPR.

An organization that determines the means of processing personal data is a controller, regardless of whether they directly collect the data from data subjects. For example, a bank (controller) collects the data of its clients when they open an account, but it is another organization (processor) that stores, digitizes, and catalogs all the information produced on paper by the bank. These companies can be datacenters or document management companies. Both organizations (controller and processor) are responsible for handling the personal data of these customers.

APPENDIX F – DATA FLOW DIAGRAMS

Data flow typically refers to the path of data from source document to data entry to processing to final reports. Data changes format and sequence (within a file) as it moves from program to program. Regarding communications, data flow is the path taken by a message from origination to destination that includes all nodes through which the data travels.

As part of an EU General Data Protection Regulation (GDPR) compliance project, organizations will need to map their data and information flows in order to assess their privacy risks. This is also an essential first step for completing a data protection impact assessment (DPIA), which is mandatory for certain types of processing.

To effectively map data flow, an organization must:

1. Understand the information flow

2. Describe the information flow. Walk through the information lifecycle to identify unforeseen or unintended uses of data. This also helps to minimize what data is collected.

3. Identify the data's key elements

4. Understand what kind of data is being processed (name, email, address, etc.) and what category does it fall into (health data, criminal records, location data, etc.)?

5. Know the data formats (hardcopy, digital, database, BYO device, mobile phones, etc.)?

6. Know your organization's data transfer methods

7. Know your organization's data collection mechanisms

8. Know the location of your data at all times.

9. Know who is accountable for the data

10. Know who has access to the data.

APPENDIX G – PRIVACY NOTICE

The EU General Data Protection Regulation (GDPR) includes rules on giving privacy information to data subjects in Articles 12, 13 and 14. These are more detailed and specific than in the DPA and place an emphasis on making privacy notices understandable and accessible. Data controllers are expected to take 'appropriate measures'.

Data controllers may need to include more information in their privacy notices, however there is still discretion for data controllers to consider where the information required by GDPR should be displayed in different layers of a notice.

The GDPR says that the information you provide to people about how you process their personal data must be:

1. Concise, transparent, intelligible and easily accessible;
2. Written in clear and plain language, particularly if addressed to a child; and
3. Free of charge.

These requirements are about ensuring that privacy information is clear and understandable for data subjects. They also make explicit what has always been set out as good practice. The explicit emphasis on adapting privacy notices for children goes beyond what is currently required by the Data Protection Act (DPA). Data controllers processing children's data will need to take account of the level of comprehension of the age groups involved and tailor their notices accordingly.

The GDPR includes a longer and more detailed list of information that must be provided in a privacy notice than the DPA does. There are also some differences in what an organization is required to provide, depending on whether you are collecting the information directly from data subjects or from a third party.