GENERAL DATA PROTECTION REGULATION

WHAT IS THE EUROPEAN UNION GENERAL DATA PROTECTION REGULATION (GDPR)?

IN 2016 THE EUROPEAN UNION (EU) RATIFIED THE GENERAL DATA PROTECTION REGULATION (GDPR) WHICH PROVIDES AN UPDATE TO THE EARLIER EUROPEAN UNION DATA PRIVACY DIRECTIVE ISSUED IN 1995. THE GDPR COMES INTO FULL EFFECT IN MAY 2018 AND IS RELEVANT NOT ONLY TO ORGANISATIONS BASED IN THE EU BUT ALSO ORGANISATIONS TRADING IN THE EU OR PROCESSING THE PERSONAL INFORMATION OF EU CITIZENS ANYWHERE IN THE WORLD. "THE AIM OF THE GDPR IS TO PROTECT ALL EU CITIZENS FROM PRIVACY AND DATA BREACHES IN AN INCREASINGLY DATA-DRIVEN WORLD THAT IS VASTLY DIFFERENT FROM THE TIME IN WHICH THE 1995 DIRECTIVE WAS ESTABLISHED. ALTHOUGH THE KEY PRINCIPLES OF DATA PRIVACY STILL HOLD TRUE TO THE PREVIOUS DIRECTIVE, MANY CHANGES HAVE BEEN PROPOSED TO THE REGULATORY POLICIES" (WWW.EUGDPR.ORG). THE EU GDPR REPRESENTS A SIGNIFICANT UPDATE TO THE PREVIOUS EU DATA PRIVACY DIRECTIVE IN THE FOLLOWING AREAS:

INCREASED TERRITORIAL SCOPE (EXTRA-TERRITORIAL APPLICABILITY)

GDPR applies to all companies processing the personal data of data subjects residing in the Union, regardless of the company's location. GDPR makes its applicability very clear - it will apply to the processing of personal data by controllers and processors in the EU, regardless of whether the processing takes place in the EU or not. The GDPR will also apply to the processing of personal data of data subjects in the EU by a controller or processor not established in the EU, where the activities relate to: offering goods or services to EU citizens (irrespective of whether payment is required) and the monitoring of behaviour that takes place within the EU. Non-EU businesses processing the data of EU citizens will also have to appoint a representative in the EU.

PENALTIES

Under GDPR, organisations in breach of GDPR can be fined up to 4% of annual global turnover or €20 million (whichever is greater). There is a tiered approach to fines e.g. a company can be fined 2% for not having their records in order (article 28), not notifying the supervising authority and data subject about a breach or not conducting impact assessment. It is important to note that these rules apply to both controllers and processors – meaning 'clouds' will not be exempt from GDPR enforcement.

CONSENT

The request for consent must be given in an intelligible and easily accessible form, with the purpose for data processing attached to that consent. Consent must be clear and distinguishable from other matters and provided in an intelligible and easily accessible form, using clear and plain language. It must be as easy to withdraw consent as it is to give it.

BREACH NOTIFICATION

Under the GDPR, breach notification will become mandatory in all member states where a data breach is likely to "result in a risk for the rights and freedoms of individuals". This must be done within 72 hours of first having become aware of the breach. Data processors will also be required to notify their customers, the controllers, "without undue delay" after first becoming aware of a data breach.

RIGHT TO ACCESS

The right for data subjects to obtain from the data controller confirmation as to whether or not personal data concerning them is being processed, where and for what purpose. Further, the controller shall provide a copy of the personal data, free of charge, in an electronic format.

BDO

RIGHT TO BE FORGOTTEN

Entitles the data subject to have the data controller erase his/her personal data, cease further dissemination of the data, and potentially have third parties halt processing of the data. Includes erasure of data no longer being relevant to original purposes for processing, or a data subject withdrawing consent.

DATA PORTABILITY

The right for a data subject to receive the personal data concerning them, which they have previously provided in a 'commonly used and machine-readable format' and have the right to transmit that data to another controller.

PRIVACY BY DESIGN

Calls for the inclusion of data protection from the onset of the designing of systems, rather than an addition. 'The controller shall…implement appropriate technical and organisational measures... in an effective way…in order to meet the requirements of this Regulation and protect the rights of data subjects'.

DATA PROTECTION OFFICERS (DPO)

DPO appointment will be mandatory only for those controllers and processors whose core activities consist of processing operations which require regular and systematic monitoring of data subjects on a large scale or of special categories of data or data relating to criminal convictions and offences.

BDO GDPR COMPLIANCE PRODUCTS

BDO GDPR Compliance Toolkit Essentials Licence: ideal for micro-sized organisations, sole trader and professional practice usage. Covers all the essentials which will support your GDPR compliance initiatives.

BDO GDPR Compliance Toolkit Core Licence: ideal for small-to-medium-sized organisations. Includes the contents of the Essentials Licence plus additional features and functionality which will support the more demanding size and complexity of your GDPR compliance initiatives.

BDO GDPR Compliance Toolkit Extended Licence: designed for enterprise-sized organisations. Includes the contents of the Core Licence plus additional features and functionality which will support the most demanding size and complexity requirements for GDPR compliance initiatives.

BDO GDPR Implementation Support Service: complements the BDO GDPR Toolkit licences. A set of pre-defined services to support your GDPR compliance preparation project.

BDO GDPR Implementation On-demand Service: designed for ad hoc support for the BDO GDPR Toolkit self-implementation option. Also for those who have completed their compliance preparation project and need additional support.

BDO GDPR Licence Updates Service: provides periodic updates to the contents of your selected BDO GDPR Toolkit Licence. Available on an optional annual contract.

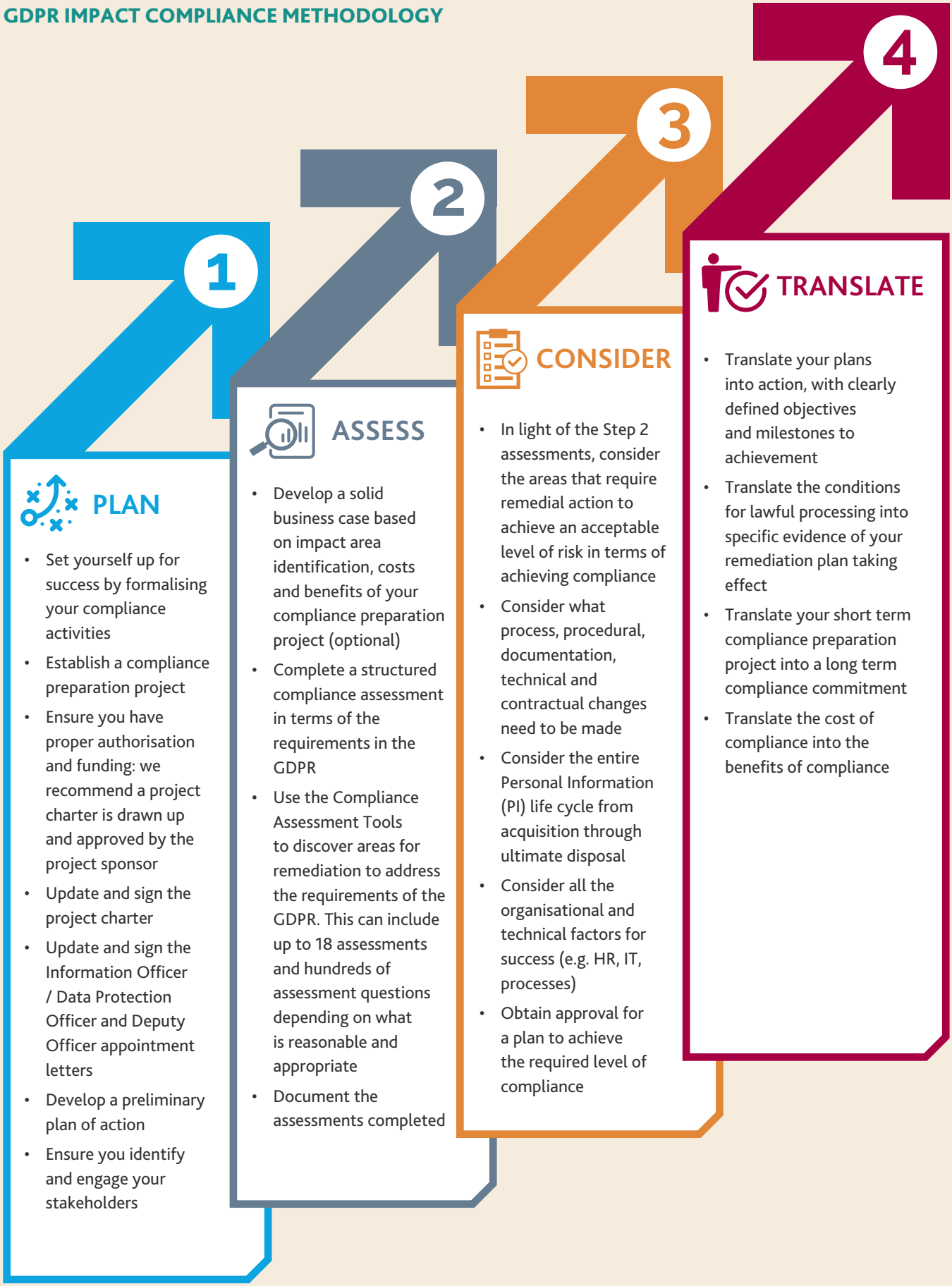
All of these BDO GDPR Compliance Toolkit Licence options are available on a self-implementation basis and can optionally be supported by our Compliance Services.

BDO SUPPORT OF ITS CLIENTS GOING THROUGH THE GDPR PROCESS

Advice and guidance on what is involved, how to achieve project tasks and what will work best based on previous projects, in the following main areas:

- The methodology specific to the GDPR project being undertaken: including assessment, risk appetite review and remediation steps in detail
- The deployment of the GDPR toolkit to achieve the project goals: how to use the tools, through formal training sessions and informal advice and coaching of the project team
- Tailoring of the tools, where necessary, to specific client needs
- Supporting the completion of assessments: ad hoc advice and guidance
- Interpretation of assessment results: helping to identify trends, anomalies, reaching valid conclusions, identifying where further assessments are required
- Analysis and synthesis of assessment results: includes report writing
- Training of project team members where necessary on the contents of the GDPR to enable them to better contribute to the project objectives
- Interpretation of legislation and regulations as far as they relate to completion of the project
- Advice to the project sponsor and project manager on GDPR technical issues which may arise
- Attending project team meetings
- Attending project steering committee meetings
- Other tasks in line with specific client requests that support project objectives

GDPR IMPACT COMPLIANCE METHODOLOGY



THE BDO 12 POINT QUICK SELF-ASSESSMENT: ARE YOU READY FOR GDPR?

ITEM HEADING	HIGH-LEVEL ADVICE	ACTION POINTS
1. Awareness	Ensure decision makers and key people in your organisation are aware that the law is changing to the GDPR and that the impact is understood.	1. Arrange a GDPR briefing for your policy makers. 2. Initiate the development of a business case for the GDPR. 3. Evaluate organisation's risk register
2. Information you hold	Document personal data that is held, where it came from and who it is shared with.	1. Use the BDO Personal Information Diagnostic Tool for an audit of personal information you hold.
3. Communicating privacy information	Review current privacy notices and devise a plan for making necessary changes in time for GDPR implementation.	1. Review your Privacy Notices using the checklist for GDPR privacy notice provided by BDO.
4. Individuals' rights	Check procedures are in place to cover all the rights individuals have, including how personal data will be deleted or how data will be provided electronically and in a commonly used format.	1. Review your existing records management processes. 2. Use the BDO Records Management Assessment Tool and Records Management Policy to support this area.
5. Subject access requests	Update procedures and plan how requests within the new time scales will be handled and what additional information will need to be provided.	1. Use the BDO Data Subject Request Log to track requests.
6. Legal basis for processing personal data	Evaluate the various types of data processing carried out, identify and document the legal basis for carrying these out.	1. Use the BDO Personal Information Diagnostic Tool for an audit of personal information you hold including the legal basis for processing.
7. Consent	Review how consent is being sought, obtained, and recorded and whether any changes need to be made.	1. Use the BDO Personal Information Diagnostic Tool for an audit of personal information you hold including the confirmation of consent. 2. Use the BDO contract templates as the basis for obtaining consent from your data subjects.
8. Children	Consider putting systems in place to verify individuals' ages and to gather parental or guardian consent for the data processing activity.	1. Use the BDO Personal Information Diagnostic Tool for an audit of personal information you hold including the processing of information on children. 2. Use the BDO contract templates as the basis for obtaining consent from parents or guardians.
9. Data breaches	Ensure the right procedures are in place to detect, report and investigate a personal data breach.	1. Use the BDO GDPR NIST Incident Response Recommendations Tool to assess your readiness for a data breach. 2. Use the BDO Security Compromise Management Guidelines when managing a data breach. 3. See supporting documents in the folder Security Compromise Management guidance in the BDO GDPR Compliance Toolkit.
10. Data Protection by Design and Data Protection Impact Assessments	Familiarise yourself with the guidance the EU has produced on Privacy Impact Assessments and evaluate how and when to implement them in your organisation.	1. Use the BDO Privacy Impact Assessment Key Questions document. 2. Review the Privacy By Design videos in the toolkit. 3. Read the ICO Privacy impact assessment code of practice in the toolkit. 4. Use the GDPR Privacy Impact Assessment Assessment template in the BDO toolkit.
11. Data Protection Officers	Designate a Data Protection Officer, if required, or someone to take responsibility for data protection compliance and assess where this role will sit within your organisation's structure and governance arrangements.	1. Appoint your Information Officer with the dual title of Data Protection Officer using the BDO appointment letter template. 2. Ensure your DPO is adequately skilled by using training available from BDO.
12. International	International organisations should determine which data protection supervisory authority your orgainsation belongs to.	1. Confirm the registered office location of your holding company or operating company. 2. Ensure you are registered with the Information Regulator for your jurisdiction. 3. Consult BDO for headquarters in other countries.

© ICO, 2017. All rights reserved

CONTACT US

Warren Glyn Carr | Manager: IT Governance and Consulting | E warren@bdo.com.na | Fax2Mail 088 61 6331 | M +264 81 129 0481