Deloitte.

General Data Protection Regulation (GDPR)

For Private circulation only

Risk Advisory

What is GDPR?
General Data Protection Regulation (GDPR) is a mandate which replaces Directive 95/46/EC and enters into application on 25th May, 2018.

What is the impact of non-compliance?

- A fine of up to €10m or 2% of the controller's annual worldwide turnover of the preceding year
- A fine of up to €20m or 4% of the controller's annual worldwide turnover of the preceding year

Does this regulation apply to organizations operating in India?
GDPR is a borderless and sector/industry independent regulation. It is expected to impact organizations across the globe that do business in Europe. The applicability of the GDPR is linked to (1) the establishment of the controller/company in the EU and (2) services provided to EU data subjects. In situations where the 'personal data' is collected outside the EU and processed outside the EU, GDPR's applicability doesn't hold.

What is the starting point in the journey of GDPR compliance?

- Assess whether your organization qualifies for GDPR
- Include privacy within the process design
- Define process and a definite purpose for an individual's interaction, record consent for the processing personal data
- Build an understanding on where the data resides and the life cycle of data within the organization
- A detailed Privacy Impact Assessment (PIA) should be undertaken and documented where 'high risk' processing takes place

What is expected from organizations once necessary controls and processes have been implemented?
Once the implementation is completed, there needs to be a robust governance design, implementation of GDPR recommendations, monitoring of adequate Data Protection controls and processes. Additionally, metrics and KPIs should be established to report on and to measure compliance with GDPR.

Our organization has a robust data protection program. Should we still be concerned about this regulation?
Yes, there are changes in GDPR which may trigger updates to privacy notice, processing based on consent, processing based on automated decision making (including profiling), access procedures (including rectification, erasure and objection) etc.

Our organization is not based in the EU. Does the Data Protection Officer provision apply to us?
Yes, if the non-EU based company is processing personal data as a consequence of:

- Offering goods or services to individuals in the EU or
- Monitoring their behaviour within the EU.
- In addition, if the core activities of your company consist of personal data processing which requires regular and systematic monitoring of individuals on a large scale

Our organization doesn't have enough scale and operations to establish a dedicated team to focus on data privacy or protection. What can be done to address this issue?
As GDPR applies to all organisations worldwide handling EU data subjects' data, it is recommended to have a GDPR strategy in place and prioritize actions in a phased and risk-based approach. If deemed non-compliant, the company may face severe penalties, and hence, should set aside resources and budget for GDPR compliance now.

Our organization has implemented a Data Leakage Protection solution. Won't that address GDPR's requirement?
As GDPR applies to all organizations worldwide handling EU data subjects, it is recommended to have a GDPR strategy in place and prioritize actions in a phased and risk-based approach.

Our organization provides testing services to organization in EU. It has access to dummy personal data, do we need to comply with GDPR?
Yes, any Organization using personal data/personal data collected in EU needs to comply with GDPR, even if it is dummy/ masked personal data.

GDPR protects data privacy rights for EU Citizens or EU residents?
Nationality or citizenship is not a factor of consideration under GDPR, it's to do with individuals whose data is processed by a controller who is subject to the GDPR. The controller or processor being in the EU is one factor, and a controller targeting EU data subjects is the other factor.

Does GDPR protect only EU Citizen personal data or any personal data (even for non-EU Citizens as well) accessed or processed or hosted by an organization having establishment in EU or its processing arm outside EU?
GDPR applies to every personal data (to be specific GDPR focuses on "personal data") that was collected within the boundaries of EU. This includes personal data from EU and non-EU data subjects. It's not a mandate to have a local office / presence in one of the EU member states is not required in order to be applicable under GDPR.

How can I "demonstrate" I am complying with the Regulation?
You will need to update or create suitable policies that set out how you process personal data. You should also consider other compliance measures, including setting up a clear compliance structure, allocating responsibility for compliance, staff training and audit. It might also involve technical measures such as minimising processing of personal data, pseudonymisation, giving individuals greater control and visibility and applying suitable security measures.

Is the fine of 4% of annual worldwide turnover calculated on a group-wide basis?
Yes. Administrative fines are applied to "undertakings" which are as defined by reference to the competition law definition in Articles 101 and 102 TFEU - Treaty on the Functioning of the European Union (2007). This views undertakings as economic units, so potentially includes group organisations.

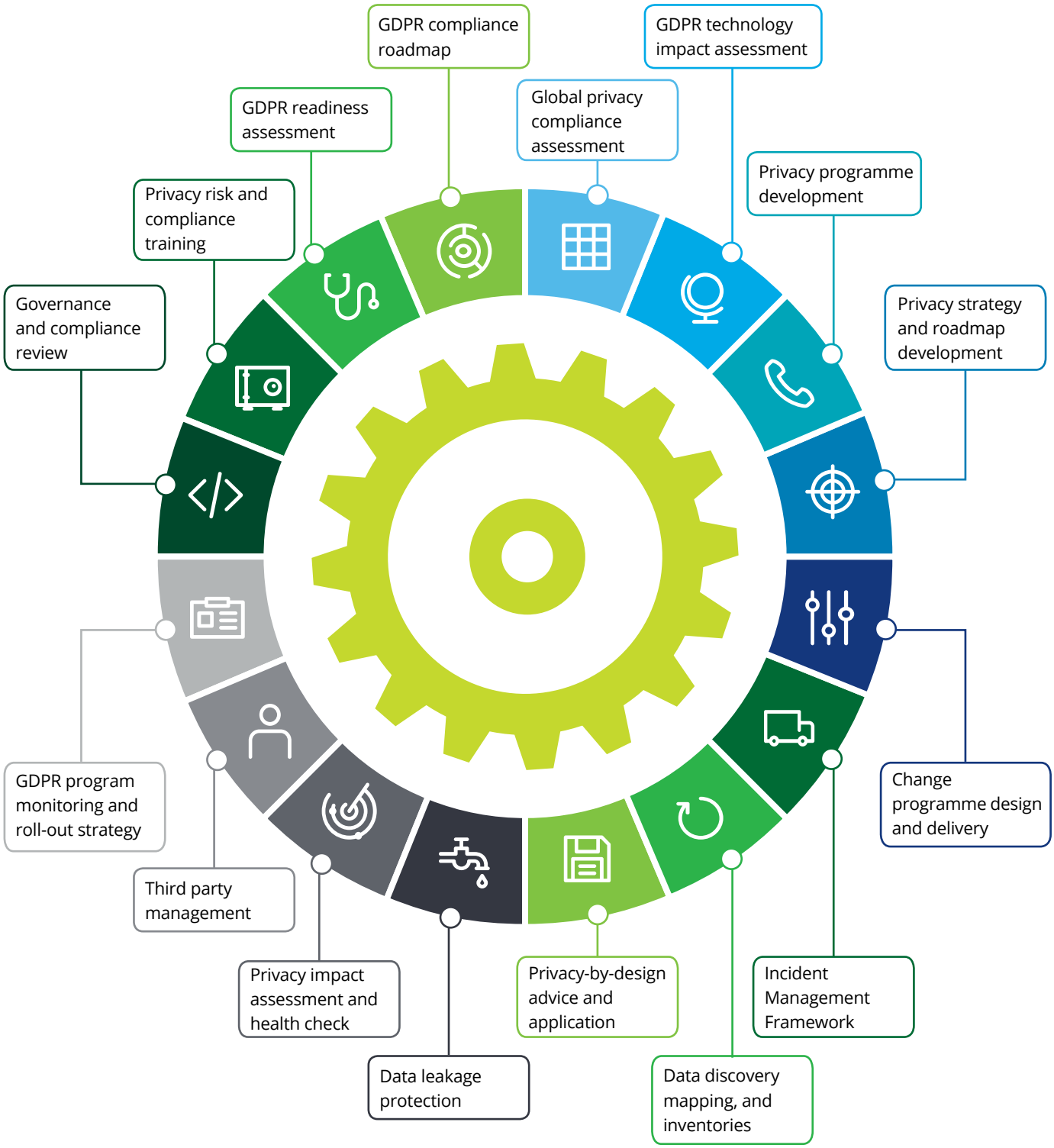
I have used Commission approved Model Contracts for years - will I have to renegotiate them?
The current Model Contracts are "grandfathered" under the Regulation until revoked or replaced. However, if you are contracting with a data processor it is not clear if the Model Contracts are sufficient to meet the new requirements in the Regulation for processor contracts, however it recommended to seek inputs / opinions from legal counsel and accordingly consider amending them as part of your general review of existing processor contracts.

Can I use the same notice across the whole of Europe? Do I need to provide my notice in a local language?
The Regulation should standardise the content of your privacy notices, but it is likely that they will still need to be translated into local languages if they are directed at a particular jurisdiction.

We can help you

Our service offering

Deloitte has a dedicated team of specialists with a deep expertise in privacy data protection programs across large scale and complex organizations, embedding change and offering a full spectrum of GDPR related services:



Contacts

Rohit Mahajan
President
Risk Advisory
rmahajan@deloitte.com

Shree Parthasarathy
Partner
Risk Advisory
sparthasarathy@deloitte.com

Manish Sehgal
Partner
Risk Advisory
masehgal@deloitte.com

Deloitte.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. Please see www.deloitte.com/about for a more detailed description of DTTL and its member firms.

This material is prepared by Deloitte Touche Tohmatsu India LLP (DTTILLP). This material (including any information contained in it) is intended to provide general information on a particular subject(s) and is not an exhaustive treatment of such subject(s) or a substitute to obtaining professional services or advice. This material may contain information sourced from ly available information or other third party sources. DTTILLP does not independently verify any such sources and is not responsible for any loss whatsoever caused due to reliance placed on information sourced from such sources. None of DTTILLP, Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the "Deloitte Network") is, by means of this material, rendering any kind of investment, legal or other professional advice or services. You should seek specific advice of the relevant professional(s) for these kind of services. This material or information is not intended to be relied upon as the sole basis for any decision which may affect you or your business. Before making any decision or taking any action that might affect your personal finances or business, you should consult a qualified professional adviser.

No entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by any person or entity by reason of access to, use of or reliance on, this material. By using this material or any information contained in it, the user accepts this entire notice and terms of use.

©2018 Deloitte Touche Tohmatsu India LLP. Member of Deloitte Touche Tohmatsu Limited