# GDPR READINESS QUESTIONS

## SCOPE AND APPLICABILITY

- Have you done the assessment as to whether your non-EU entities will be subject to the GDPR?
- Do any of your non-EU entities offer goods or services directly to EU residents?
- Have you determined whether you 'monitor behavior'? According to what criteria?
- Have you considered changing any of your systems/processes in order to avoid applicability of the GDPR?

## NOTICES

- How many notices do you have (employee, website, customer)?
- Do you have a global notice or do you use localized notices?
- If localized notices, do you use templates that you make available on a local level?
- Do you have a process in place to update the notices
- Do you have a process to roll out the updated notices?

## LEGAL BASIS/CONSENT

- In what aspects of your business do you rely on consent?
- Have you considered whether the other legal bases might be sufficient such that consent won't be needed?
- Have you considered the broader scope of legitimate interest as an alternative legal basis?
- Do you document the legal basis on which you rely?

## DATA RETENTION/DELETION

- Do you have a data retention/data deletion policy and process?
- Is it global or local?
- Has the data retention policy been implemented?
- Do you have automated deletion practices?

MORRISON FOERSTER

## THIRD PARTY CONTRACTS

- Do you use templates for third party contracting?
- Are these maintained globally or locally?
- Do you have a plan for a process to update agreements with service providers?
- Do you have a plan for a process to respond to update requests to agreements with customers?
- Have you thought about how you will interact with your customers if you believe an instruction is unlawful?

## THIRD PARTY DUE DILIGENCE

- Do you engage in third party due diligence that includes checking criminal data?
- Do you conduct those reviews in a centralized manner or locally?

## ACCOUNTABILITY

- Do you already have a written program that could serve as privacy compliance program?
- What compliance features do you already have in place that could be leveraged towards a compliance program?
- Does internal audit, audit the privacy program?
- Do you have a cross functional governance committee and privacy points of contacts in the business?
- Do you have written policies and procedures that are consistent with GDPR that can be leveraged?
- Do you have a plan in place to update those policies and procedures?

## PRIVACY BY DESIGN

- Do you have a centralized process for developing new products and services?
- Do you have a centralized process for acquiring/procuring new products and services?
- Do you have a process to consider issues such as key-coding techniques, data minimization, limiting access, data retention prior to a product/service being launched?
- Do you have a product/service development go-live process that would allow for privacy by design to be incorporated as 'development gate'?

## RECORDKEEPING/INVENTORY

- How do you currently deal with regulator registrations/notifications?
- With which group does that obligation currently reside (the business/privacy/compliance)?
- Do you have a centralized view of the existing registrations?
- Have you thought about how you will handle the documentation process (within IT, within Privacy, global vs. local, new projects vs. existing processes)
- Who will be responsible for complying with the Article 30 record-keeping/inventory obligation?
- Have you identified a tool that can be used to support the documentation obligation?

## DATA PRIVACY IMPACT ASSESSMENT

- Do you engage in large scale processing of sensitive data? Criminal data?
- Do you engage in systematic monitoring of publically accessible places?
- Do you currently have any PIA process?
- How do you document mitigating controls?
- Do you have a plan in place to create a DPIA process?

## DATA PROTECTION OFFICER

- Do you engage in the systematic monitoring of individuals?
- Do you engage in large scale processing of sensitive data? Criminal data?
- Do you have an existing Data Protection Officer (Global/Europe)?
- Do you intend to put a DPO in place?

## CROSS-BORDER TRANSFERS

- How have you currently addressed your cross-border transfers?
- What mechanisms are in place to move European Data cross border?

## TRAINING AND AWARENESS?

- Do you currently have privacy awareness training for the general population?
- Do you have any targeted training for high risk groups (HR, IT, Finance)?

## BREACH NOTIFICATION

- Do you have an incident response plan? Do you train on it?
- Is it global or local?
- Do you need to change anything to meet the 72 hour obligation?

## INDIVIDUAL'S RIGHTS

- How are your processes for dealing with access requests currently set up?
- Are they centralized / decentralized?
- Would there be a need to specifically change the processes to cater for new rights (RTBF, right to objection, portability etc.)?
- How likely is it that customers/employees will exercise RTBF requests? Data portability requests?
- Do you have a plan in place to support requests from corporate customers to assist them in meeting their obligation to respond to individual rights requests?

## PROFILING

- Do any of your processes involve automated decision making or decision making based on analytics?
- If so, is this done in a way that could affect people? How are the outcomes of the processes applied? Are the processes and the outcomes reviewed by a person?