UNDERSTANDING MICROSOFT'S SSPA APPLICABILITY AND DPR

It is highly likely that if you play in the Information Technology space you either use or may provide services to Microsoft. Alternatively, if you have an opportunity to become a Supplier to Microsoft Corporation then you will need to established a Security and Data Assurance baseline.

Scope – Data involved

Microsoft's in-house developed Supplier Security and Privacy Assurance (SSPA) program is an annual requirement once you become an active Microsoft supplier. The scope of the SSPA covers all suppliers globally that process Personal Data and/or Microsoft Confidential Data in connection with any active Master Service Agreement (MSA), Statement of Work (SOW) or Purchase Order (PO).

Data types across Microsoft are extensive and the program has been developed to accommodate all data use cases, whilst taking into account global regulation, companies across all industry types and suppliers of all various sizes, small startups to multi-conglomerates. No mean feat.

Applicability

Whether you are well into your Governance, Risk and Compliance (GRC) journey or maturing enough that clients are asking for some level of assurance, this program is a great way to establish a strong baseline. The key to any supplier compliance program is defining what information is needed and being collected. MSFT's SSPA requires you to establish your "Applicability" and then have it independently assessed against their Data Protection Requirements (DPR).

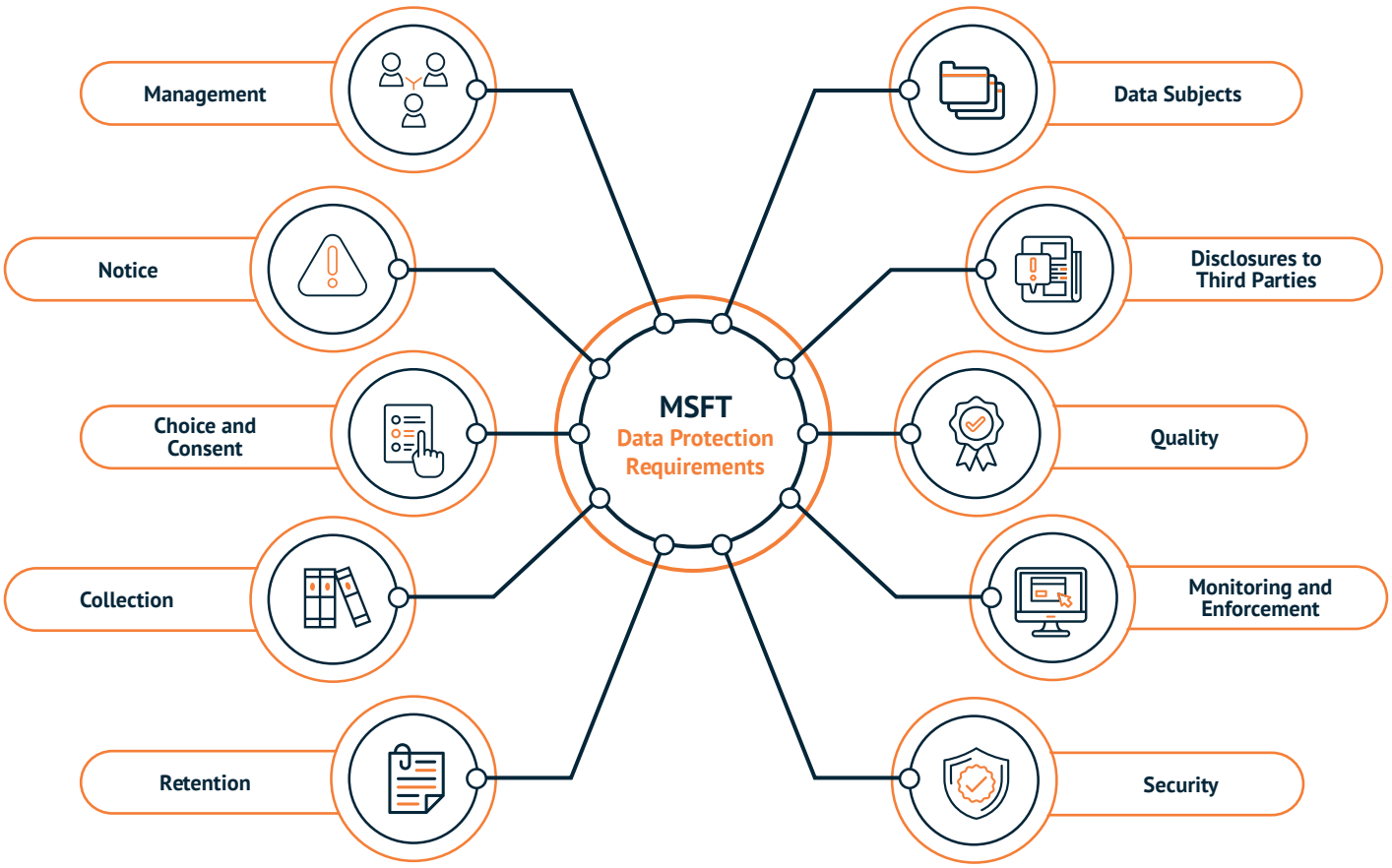
Data Protection Requirements

The DPR is made up of 10 categories which follow a Data Governance lifecycle model. Its very similar to the Gramm-Leach-Bliley Act (GLB Act or GLBA) and has elements of the EU:GDPR requirements but most importantly has MSFT MSA contractual terms and conditions woven in.

At a high level the principles are:

- MSFT Data can only be used in accordance to or as intended via an active and approved MSA.
- MSFT employees or MSFT affiliates must be notified of data sharing between financial institutions and third parties and have the ability to opt in/out of private information sharing.
- Data Subject Rights must be established and actionable in a timely manner
- MSFT Data must be secured against unauthorized access.
- User activity must be tracked, including any attempts to access protected records.
- Suppliers must have an incident response plan and both Security and Data Privacy training.

You can see the 10 Categories listed in the diagram below.



Additionally, MSFT categorizes your organization via a SSPA Data Processing Profile which is self-managed via the Aravo Supplier Portal. Navigating this portal can be challenging but it is important to track your status; Active Green (compliant) vs Suspended Red (non-compliant) and to comply to tasks which are issued with a 90 day compliance deadline.

SSPA Independent Assessment

If you just received your notification from MSFT or need assistance with known gaps or remediation, Connor's Global team can provide clear guidance to setup your GRC and supplier program. We have an extensive library of Policy and Procedures you can leverage and adopt to move you to a stronger Security and Data Privacy baseline.

Connor has expertise in Microsoft's SSPA program "Applicability", the Data Protection Requirements and core policy and procedure documents needed to successfully pass this assessment. We are a compliance specialty firm with a proven record and global presence.