Actualización de la Política Global de Privacidad de MetLife con aspectos regulatorios locales

Argentina

Este documento forma parte de Política Global de Privacidad de MetLife emitida por la Oficina Corporativa de Privacidad) de MetLife. La presente información sobre Consideraciones locales ha sido revisada y autorizada por la Oficina Corporativa de Privacidad

A lo largo de este documento se definen los criterios aplicables en Argentina con base en su regulación local y que se consideran **adicionales a la Política Global.**

INTRODUCCIÓN

El prestigio como así también la información creada, procesada y utilizada por MetLife y sus empresas vinculadas, es uno de nuestros activos más valiosos. Considerando la naturaleza competitiva de nuestras Compañías y el significativo valor de los recursos que manejamos, será nuestra obligación proteger estos activos en concordancia con los riesgos del negocio.

Comprometer nuestro prestigio y los activos de información puede impactar severamente sobre nuestros Clientes y Empleados, constituir una violación a las leyes y regulaciones vigentes, y afectar negativamente la reputación, la imagen y los resultados económicos de nuestras Compañías y de la Corporación.

El presente documento establece los tipos de información que requieren protección dentro de la Compañía, y el tratamiento que se le debe prestar a la misma.

La presente política tiene por objeto la protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean éstos públicos, o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre, de conformidad a lo establecido en el artículo 43, párrafo tercero de la Constitución Nacional.

I. PERSPECTIVA GENERAL

1. Ley aplicable

El marco regulatorio que rige al país en materia de privacidad de la información, comprende:

- ✓ La Ley 25.326 de Habeas Data.
- ✓ El Decreto Reglamentario 1.558/01.
- ✓ Disposiciones de la Dirección Nacional de Protección de Datos Personales (DNPDP).
  - o Disposición 4/2009
    Avisos con fines de publicidad directa. Aviso al titular de los datos sobre su derecho de retiro o bloqueo parcial.
  - o Disposición 10/2008

Inclusión en la página Web y en los documentos de captura de datos sobre los derechos del titular de los datos.

- Disposición 11/2006
  Medidas de seguridad para el tratamiento y conservación de datos personales.

2. Responsable

La figura del Data Privicay Officer no es requerida por la regulación local. La ley solo reauiere que sea designado un responsable de las bases de datos registradas.

3. Definiciones

- ✓ **Datos personales:** Información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables.

- ✓ **Datos sensibles**: Datos personales que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual.

- ✓ **Archivo, registro**, base o banco de datos: Indistintamente, designan al conjunto organizado de datos personales que sean objeto de tratamiento o procesamiento, electrónico o no, cualquiera que fuere la modalidad de su formación, almacenamiento, organización o acceso.

- ✓ **Tratamiento de datos:** Operaciones y procedimientos sistemáticos, electrónicos o no, que permitan la recolección, conservación, ordenación, almacenamiento, modificación, relacionamiento, evaluación, bloqueo, destrucción, y en general el procesamiento de datos personales, así como también su cesión a terceros a través de comunicaciones, consultas, interconexiones o transferencias.

- ✓ **Responsable de archivo, registro, base o banco de datos**: Persona física o de existencia ideal pública o privada, que es titular de un archivo, registro, base o banco de datos.

- ✓ **Datos informatizados:** Los datos personales sometidos al tratamiento o procesamiento electrónico o automatizado.

- ✓ **Titular de los datos:** Toda persona física o persona de existencia ideal con domicilio legal o delegaciones o sucursales en el país, cuyos datos sean objeto del tratamiento al que se refiere la presente ley.

- ✓ **Usuario de datos:** Toda persona, pública o privada que realice a su arbitrio el tratamiento de datos, ya sea en archivos, registros o bancos de datos propios o a través de conexión con los mismos.

- ✓ **Disociación de datos:** Todo tratamiento de datos personales de manera que la información obtenida no pueda asociarse a persona determinada o determinable.

4. Calidad de los datos (clasificación de la información)

- ✓ Los datos personales que se recojan a los efectos de su tratamiento deben ser ciertos, adecuados, pertinentes y no excesivos en relación al ámbito y finalidad para los que se hubieren obtenido.

- ✓ La recolección de datos no puede hacerse por medios desleales, fraudulentos o en forma contraria a las disposiciones de la presente ley.

- ✓ Los datos objeto de tratamiento no pueden ser utilizados para finalidades distintas o incompatibles con aquéllas que motivaron su obtención.

- ✓ Los datos deben ser exactos y actualizarse en el caso de que ello fuere necesario.

- ✓ Los datos total o parcialmente inexactos, o que sean incompletos, deben ser suprimidos y sustituidos, o en su caso completados, por el responsable del archivo o base de datos cuando se tenga conocimiento de la inexactitud o carácter incompleto de la información de que se trate, sin perjuicio de los derechos del titular establecidos en el artículo 16 de la presente ley.

- ✓ Los datos deben ser almacenados de modo que permitan el ejercicio del derecho de acceso de su titular.

- ✓ Los datos deben ser destruidos cuando hayan dejado de ser necesarios o pertinentes a los fines para los cuales hubiesen sido recolectados.

5. Categoría de los datos

- ✓ Ninguna persona puede ser obligada a proporcionar datos sensibles.

- ✓ Los datos sensibles sólo pueden ser recolectados y objeto de tratamiento cuando medien razones de interés general autorizadas por ley. También podrán ser tratados con finalidades estadísticas o científicas cuando no puedan ser identificados sus titulares.

- ✓ Queda prohibida la formación de archivos, bancos o registros que almacenen información que directa o indirectamente revele datos sensibles. Sin perjuicio de ello, la Iglesia Católica, las asociaciones religiosas y las organizaciones políticas y sindicales podrán llevar un registro de sus miembros.

- ✓ Los datos relativos a antecedentes penales o contravencionales sólo pueden ser objeto de tratamiento por parte de las autoridades públicas competentes, en el marco de las leyes y reglamentaciones respectivas.

6. Actualización, rectificación y supresión de la información

Aspectos regularorios

- ✓ Toda persona tiene derecho a que sean rectificados, actualizados y, cuando corresponda, suprimidos o sometidos a confidencialidad los datos personales de los que sea titular, que estén incluidos en un banco de datos.

- ✓ El responsable o usuario del banco de datos, debe proceder a la rectificación, supresión o actualización de los datos personales del afectado, realizando las operaciones necesarias a tal fin en el plazo máximo de cinco días hábiles de recibido el reclamo del titular de los datos o advertido el error o falsedad.

- ✓ El incumplimiento de esta obligación dentro del término acordado en el inciso precedente, habilitará al interesado a promover sin más la acción de protección de los datos personales o de hábeas data prevista en la presente ley.

- ✓ En el supuesto de cesión, o transferencia de datos, el responsable o usuario del banco de datos debe notificar la rectificación o supresión al cesionario dentro del quinto día hábil de efectuado el tratamiento del dato.

- ✓ La supresión no procede cuando pudiese causar perjuicios a derechos o intereses legítimos de terceros, o cuando existiera una obligación legal de conservar los datos.

- ✓ Durante el proceso de verificación y rectificación del error o falsedad de la información que se trate, el responsable o usuario del banco de datos deberá o bien bloquear el archivo, o consignar al proveer información relativa al mismo la circunstancia de que se encuentra sometida a revisión.

- ✓ Los datos personales deben ser conservados durante los plazos previstos en las disposiciones aplicables o en su caso, en las contractuales entre el responsable o usuario del banco de datos y el titular de los datos.

Procedimiento

El proceso de destrucción de la información de la Compañía es tan importante como la correcta clasificación de la misma. Desde el momento en que todos los esfuerzos son canalizados a proteger nuestra información de accesos o divulgaciones no autorizados, en el mismo sentido debemos prestar la máxima atención para establecer mecanismos que nos permitan destruir la información de manera segura, previniendo posibles accesos no deseados. Para ello será necesario tener en consideración los siguientes tópicos:

a) Información en Papel / Carpetas / Legajos / Expedientes

- Toda la información deberá ser destruida al final de su ciclo de vida, contemplando los plazos legales de la misma y cumpliendo con los lineamientos del "Record Information Management" (RIM) disponible en la base de Normas y Procedimientos. Cualquier consulta asociada al ciclo de vida por tipo de documento deberá ser canalizada a través de la Dirección de Legales.
- Los reportes y/o documentos clasificados con niveles de seguridad Medios o Críticos que vayan a ser destruidos, no deben ser dejados por ningún motivo sobre el piso, escritorios, pasillos, escaleras, ni en dispositivos de basura. Todos estos materiales deberán ser destruidos inmediatamente o depositados en los contenedores de destrucción de información provistos por la Compañía (sistema Shred-it). En caso de no existir este servicio (como por ejemplo en las Agencias) se procederá, bajo la supervisión del responsable del área o de la Agencia, a la destrucción manual de dicha documentación de tal manera que no sea posible volver a reconstruir la documentación ya destruida.
- En caso de no poder realizar la destrucción de la información de manera inmediata, todo reporte o documento pendiente de destrucción deberá ser protegido hasta el momento de efectivizar la misma. Dicho proceso deberá realizarse tan pronto como sea posible.
- Si bien la responsabilidad final por el correcto cumplimiento de estos procedimientos es de los Responsables de cada área, todos los Empleados de la Compañía y personal contratado son responsables por la información que la Compañía administra.

b) Información en Medios Digitales

- El proceso de destrucción de medios magnéticos deberá realizarse de acuerdo con lo expresado en el instructivo "Destrucción de Dispositivos de Grabación y de Equipos Informáticos" (existente en la base de Normas y Procedimientos).

II. AVISO, CONSENTIMIENTO Y CONTROL

1. Información

Aspectos regularorios

Cuando se recaben datos personales se deberá informar previamente a sus titulares en forma expresa y clara:

- ✓ La finalidad para la que serán tratados y quiénes pueden ser sus destinatarios o clase de destinatarios;
- ✓ La existencia del archivo, registro, banco de datos, electrónico o de cualquier otro tipo, de que se trate y la identidad y domicilio de su responsable;
- ✓ El carácter obligatorio o facultativo de las respuestas al cuestionario que se le proponga, en especial en cuanto a los datos referidos en el artículo siguiente;
- ✓ Las consecuencias de proporcionar los datos, de la negativa a hacerlo o de la inexactitud de los mismos;
- ✓ La posibilidad del interesado de ejercer los derechos de acceso, rectificación y supresión de los datos.

Procedimiento

En todos aquellos casos en que MetLife colecte datos personales de sus Clientes, se le debe notificar de sus derechos sobre sus datos según los establece la Disposición 10/2008 mencionada en el punto 1.3 (Aspectos regulatorios). Esto incluye los que se requieren:

a) a través de las solicitudes de pólizas por las características propias de la contratación del seguro
b) en las Solicitudes de denuncias de siniestros o de rescates
c) en las Solicitudes de actualización de datos del Cliente o de los Beneficiarios
d) con fines de captación de datos con objetivos comerciales por cualquier medio, internet o campañas de marketing en eventos o en la vía pública.

El responsable del área de **Marketing** deberá asegurar la inclusión en la documentación o medios mencionados en los puntos que anteceden, de la siguiente notificación al Cliente:
"El titular de los datos personales tiene la facultad de ejercer el derecho de acceso a los mismos en forma gratuita a intervalos no inferiores a seis meses, salvo que se acredite un interés legítimo al efecto conforme lo establecido en el artículo 14, inciso 3 de la Ley N° 25.326. La DIRECCIÓN NACIONAL DE PROTECCIÓN DE DATOS PERSONALES, Órgano de Control de la Ley N° 25.326, tiene la atribución de atender las denuncias y reclamos que se interpongan con relación al incumplimiento de las normas sobre protección de datos personales"

Corresponde a la **Dirección de Legales** y a la **Gerencia de Ethics & Compliance** asegurar la inclusión de la presente notificación al Cliente, dentro del proceso de aprobación de Material de Venta.

2. Consentimiento

- ✓ El tratamiento de datos personales es ilícito cuando el titular no hubiere prestado su consentimiento libre, expreso e informado, el que deberá constar por escrito, o por otro medio que permita se le equipare, de acuerdo a las circunstancias.

- ✓ El referido consentimiento prestado con otras declaraciones, deberá figurar en forma expresa y destacada, previa notificación al requerido de datos.

No será necesario el consentimiento cuando:

- ✓ Los datos se obtengan de fuentes de acceso público irrestricto;

- ✓ Se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal;

- ✓ Se trate de listados cuyos datos se limiten a nombre, documento nacional de identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento y domicilio;

3. Derecho de acceso

- ✓ El titular de los datos, previa acreditación de su identidad, tiene derecho a solicitar y obtener información de sus datos personales incluidos en los bancos de datos públicos, o privados destinados a proveer informes.

- ✓ El responsable o usuario debe proporcionar la información solicitada dentro de los diez días corridos de haber sido intimado fehacientemente. Vencido el plazo sin que se satisfaga el pedido, o si evacuado el informe, éste se estimara insuficiente, quedará expedita la acción de protección de los datos personales o de hábeas data prevista en esta ley.

- ✓ El derecho de acceso a que se refiere este artículo sólo puede ser ejercido en forma gratuita a intervalos no inferiores a seis meses, salvo que se acredite un interés legítimo al efecto.

- ✓ El ejercicio del derecho al cual se refiere este artículo en el caso de datos de personas fallecidas le corresponderá a sus sucesores universales.

III. PROTECCION DE LA INFORMACIÓN

Aspectos regularorios

- ✓ El responsable o usuario del archivo de datos debe adoptar las medidas técnicas y organizativas que resulten necesarias para garantizar la seguridad y confidencialidad de los datos personales, de modo de evitar su adulteración, pérdida, consulta o tratamiento no autorizado, y que permitan detectar desviaciones, intencionales o no, de información, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado.

- ✓ Queda prohibido registrar datos personales en archivos, registros o bancos que no reúnan condiciones técnicas de integridad y seguridad.

Política de Escritorios Limpios

Se encuentra publicada y a disposición de todos los empleados la Política de Resguardo de Información en Escritorios cuyo objeto es e stablecer la política de resguardo de reportes que contengan información personal, confidencial o restringida, con el fin de reducir los riesgos de acceso no autorizado, daño o pérdida de información para la compañía.

- La clasificación de la información administrada por cada sector, será responsabilidad de los **Responsables de cada área de negocio** según las características y naturaleza de la misma.

- Todos los Empleados de la Compañía deben asegurarse que la oficina a la que pertenecen, quede en condiciones ordenadas al finalizar la jornada de trabajo. Todos los escritorios, muebles, y cualquier otra superficie debe quedar libre de materiales con información clasificada con niveles de seguridad CRÍTICO y MEDIO, independientemente del medio en el cual se encuentre almacenada.

- Los **Responsables de cada área** deberán asegurar la existencia de medios aptos para el resguardo y almacenamiento de la información de nivel CRÍTICA y MEDIO (gabinetes cerrados, cajas ignífugas, salas de archivo). En caso que se decidiera, se podrá etiquetar la documentación a nivel de carpetas, expedientes o legajos siempre y cuando estos medios se manejen como un todo y sus partes componentes no sean removidas por separado.

- Todo contrato con Proveedores externos deberá incluir una cláusula de confidencialidad y otra relacionada con la destrucción de la información luego de su procesamiento / uso.

- En referencia a la información almacenada digitalmente, las políticas de seguridad de **IT** más relevantes (existentes en la base de Normas y Procedimientos) son:

  a) **Seguridad de Datos** - Estándar de IT

  b) **Administración de Seguridad** - Estándar de IT

  c) **Revelación de Información Confidencial de MetLife** - Política de IT

  d) **Recibir Información Confidencial de Terceros** - Política de IT

Importante: La regulación local no establece la obligación de proteger la información remitidas por medios electrónicos con herramientas tecnológicas como “Envío seguro”

IV. PROCESAMIENTO DE DATOS PARA TERCEROS

- ✓ Cuando por cuenta de terceros se presten servicios de tratamiento de datos personales, éstos no podrán aplicarse o utilizarse con un fin distinto al que figure en el contrato de servicios, ni cederlos a otras personas, ni aun para su conservación.

- ✓ Una vez cumplida la prestación contractual los datos personales tratados deberán ser destruidos, salvo que medie autorización expresa de aquel por cuenta de quien se prestan tales servicios cuando razonablemente se presuma la posibilidad de ulteriores encargos, en cuyo caso se podrá almacenar con las debidas condiciones de seguridad por un período de hasta dos años.

Evalución del terceso - etapas a seguir

Para cada nuevo contrato o acuerdo y por la renovación de los existentes se deben seguir los 3 pasos de evaluación definidos en detalle en la Políticga Globla de Privacidad actualizada a Marzo 2017.

Los 3 pasos a seguir son:

a) Completar una evaluación de riesgo prelimianar.
Llevada Adelante por la línea de negocios que origina la necesidad de la contratación o renovación. Debe evluarse el riesgo de privacidad considerando si el tercero manejará datos del personal de MetLife, de clientes o de futuros clientes.

b) Completar el proceso de "Debida Diligencia" sobre el tercero.
Conducir una evaluación de seguridad del tercero a efectos de obtener aseguramiento de la protección de los datos a administrar. El proceso es conducido con el área de Riesgos de Tecnología según se define en la Política Global.

c) Incluir determinadas cláusulas en el acuerdo firmado sobre Confidencialidad y Protección de Datos.

El área legal debería incluir como mínimo las siguientes cláusulas.

- ✓ Cumplimiento de disposiciones regulatorias.
- ✓ Explicitar el propósito a dar a los datos utilizados.
- ✓ Cláusulas que aseguren la protección de la información desde los estándares de tecnología.
- ✓ Claúsulas de no divulgación de la información a terceros, salvo que sea requerido por motivos judiciales.
- ✓ Tiempo de retención de la información o documentación y su posterior destrucción.
- ✓ Obligación de notificar a MetLife por incidentes de seguridas ocurridos.
- ✓ Cláusulas sobre la subcotnratación de los servicios y la necesidad de que la misma sea aprobada por MetLife.
- ✓ Derecho de auditoría por parte de MetLife.

V. TRANSFERENCIAS TRANSFRONTERIZAS DE DATOS

Aspectos regularorios

a) Es prohibida la transferencia de datos personales de cualquier tipo con países u organismos internacionales o supranacionales, que no proporcionen niveles de protección adecuados.

b) La prohibición no regirá en los siguientes supuestos:

- ✓ Colaboración judicial internacional;

- ✓ Intercambio de datos de carácter médico, cuando así lo exija el tratamiento del afectado, o una investigación epidemiológica aplicando procedimientos de disociasión de la información.

- ✓ Transferencias bancarias o bursátiles, en lo relativo a las transacciones respectivas y conforme la legislación que les resulte aplicable;

- ✓ Cuando la transferencia se hubiera acordado en el marco de tratados internacionales en los cuales la República Argentina sea parte;

- ✓ Cuando la transferencia tenga por objeto la cooperación internacional entre organismos de inteligencia para la lucha contra el crimen organizado, el terrorismo y el narcotráfico.

Procedimiento

La transferencia de datos fuera del país para su tratamiento dentro de los procesos de gestión del negocio o por aspectos regulatorios (por ejemplo: cruce con listas antiterroristas, administración de recursos humanos), deberá estar respaldada por la firma de un acuerdo escrito donde queden resguardados los datos personales suministrados, el fin para el que van a ser utilizados y el cumplimiento de las regulaciones locales referidas a la materia.

La firma y guarda de los acuerdos mencionados es responsabilidad de la **Dirección de Legales**, siendo supervisado el cumplimiento por la **Gerencia de Ethics & Compliance**.

En todos aquellos casos mencionados y en cumplimiento del punto 2.6 del presente procedimiento, se incluirá la notificación mencionada más abajo donde el Cliente otorga su consentimiento para uso de datos personales y su transferencia al exterior.
"*Transferencia de datos al exterior/terceros - Consentimiento para uso de datos personales*". *Con la firma del presente documento me notifico y doy mi consentimiento a MetLife Seguros S.A. / MetLife Seguros de Retiro S.A. (según corresponda) para compartir todos los datos personales contenidos en la presente, los datos personales generados por la relación, y en los sucesivos que suscriba con dicha Aseguradora, con sus empresas relacionadas, afiliadas, subsidiarias, empresas, terceros –sean personas públicas o privadas- y/o con personas que auxilien tanto a la operación y administración de esta póliza, así como a la comercialización de sus productos y servicios, la que tendrá por objeto servir para efectos estadísticos, referencias comerciales, ofertas de marketing, cumplimiento de disposiciones legales, y/o para propender a mejorar la calidad del servicio. Asimismo me notifico y consiento la posibilidad de que esos datos sean transferidos, con idénticos fines, al exterior -a personas tanto públicas como privadas-, incluyendo a países que no tengan una ley idéntica a la ley de protección de datos de Argentina sin perjuicio de lo cual entiendo que se mantiene mi derecho de acceso y corrección de los datos personales.*

VI. ADMINISTRACIÓN DE INCIDENTES DE DATOS PERSONALES

Aspectos regularorios

Los incidentes o la fuga de datos personales no se encuentra explícitamente definida en la regulación loca.

Procedimiento Interno.

Un Incidente de Datos Personales ocurre cuando información personal ha sido o existe la posibersonales" lidad que sea trasmitida o puesta a disponición de alguien que no debería tener acceso a la misma.

El procedimiento de identificación del incidente y los pasos a seguir se encuentran descriptios en el procedimiento **"Manejo del Incidente de Datos Personales"** a efectos de responder apropiadamente.

Paso 1
Reportarlo al responsable local de Etica y Cumplimiento

Paso 2
Identificar los datos personales sujetos al incidente e investigar las causas y el alcance
Paso 3
A partir de la investigación, definir si se trata de un incidente de fuga de datos o solo un incidente que involucra o puede involucrar datos personales pero no su conocimiento a terceros.

Paso 4
Evaluar con la Dirección Legal el incidente y si el mismo debe ser reportado a terceros.

Paso 5
Notificarlo al "Corporate Privacy Officer" si se cumplen con los supuestos definidos en el procedimiento.

Paso 6
Mantener toda la documentación y datos referidos a la investigación realizada.

Documentación del proceso de investigación

El proceso de investigación del incidente o de la fuga de datos personales será conducido dentro del protocolo de investigación seguido por Etica y Cumplimiento, identificando según los estándadares de Auditoría Intera:

- ✓ Origen del incidente
- ✓ Universo y personal afectado pudiendo ser caratulado como fraude de ser necesario y dando intervención a Recusrsos Humanos.
- ✓ Impacto
- ✓ Posibles consecuencias legales
- ✓ Conclusión y definición de los planes de acción necesarios.

VII. EVALUACIÓN DEL IMPACTO

La normativa local no exige evaluación del impacto de los nuevos proyectos sobre las reglas de privacidad en el manejo de información personal o sensible.

VIII. CAPACITACIÓN

El Privacy Champion será el responsable de:

- ✓ Identificar las necesidades capacitación de los empleados
- ✓ Brindar capacitación a los empleados
- ✓ Mantener registros de todas las actividades de capacitación
- ✓ Obtener la aprobación de la Oficina Corporativa de Privacidad en caso de modificar significativamente los materiales de capacitación con respecto a la política global de Privacidad.

En tanto que Cumplimiento local validará el cumplimiento sobre la capacitación a los empleados, así como confirmar sobre el mantenimiento de registros de todas las actividades de capacitación.

IX. FUSIONES Y ADQUISICIONES

En caso de existir alguna adquisición o venta de negocios, el departamento Legal en conjunto con Cumplimiento local y el Gerente de Privacidad definirán el alcance de la debida diligencia en materia de privacidad.

Anexo I

Appendix A: Privacy Risk Checklist for Third Parties

MetLife is committed to protecting the security, confidentiality and integrity of its customers' and employees' personal information, as well as complying with the privacy and data protection laws of each country in which the company conducts business. MetLife may be held responsible for the acts of a third party if the personal information of MetLife customers or employees is compromised while performing services for or on behalf of MetLife. To mitigate the risk of doing business with third parties processing MetLife customer or employee personal information, the relevant line of business or functional area must complete the following checklist for every new engagement with a third party and every existing engagement that will be renewed. Once completed, the head of the relevant line of business or functional area must certify to the accuracy of the checklist responses and actions taken.

Question 1: Will the third party, or a subcontractor of the third party, collect, access, share, use, view, or store the personal information of MetLife employees, existing customers, or potential customers?	☐ Yes ☐ No
Question 2: Will the third party, or a subcontractor of the third party, conduct marketing on behalf of MetLife using the personal information of MetLife employees, existing customers, or potential customers?	☐ Yes ☐ No
If the answer to Questions 1 and/or 2 is "Yes," then you <u>must</u> complete (a), (b), (c), and (d) below	
(a) Contact IT Risk & Security at ARS_MOREs@metlife.com to conduct due diligence on the third party's information security and data protection practices.	☐ *Check this box to confirm that IT Risk & Security has been engaged to conduct due diligence of the third party.*
(b) Work with the Law Department to include privacy and data protection provisions into the third party agreement, contract, or purchase order.	☐ *Check this box to confirm that the Law Department has been engaged to include privacy and data protection provisions in the agreement.*
(c) From which country/countries will the personal information originate?	

(d) In which country/countries will the personal information be viewed, stored, processed, or accessed? ***Note:*** *Processing personal information is broadly defined to include any operation performed on the information such as viewing, collecting, storing, altering, retrieving, using, transferring, disclosing, disseminating, blocking, erasing or destroying.*	
If the countries identified in response (c) and (d) are different, then you must work with the Law Department to determine whether a data transfer agreement or other transfer mechanism is required under applicable law or regulation. ***Note:*** *Absent legal restrictions, there may be contractual limitations on where data may be stored or accessed. You should work with the line of business that maintains the business relationship with the data to address any contractual limitations that may apply.*	☐ *Check this box to confirm that the Law Department has been engaged to assess cross-border data transfer legal requirements.*

I certify that the answers provided in this checklist are accurate and complete to the best of my knowledge, and that prior to engaging the third party I have completed all actions required of me under the Global Privacy Policy, including where required: (i) working with IT Risk & Security to complete due diligence on the third party; and (ii) working with the Law Department to include appropriate privacy and data protection provisions in the agreement, as well as to ensure the appropriate cross-border data transfer mechanism is in place as required by applicable local law.

Name of person completing this form

Signature

Date

Name of Line of Business/Function Head

Signature

Date