Global Privacy & Information Security Program

2022

MetLife

Contents

Overview

MetLife has a long-standing commitment to privacy and information security.

MetLife, Inc. operates worldwide through subsidiaries, affiliates, branches, and joint ventures (collectively "MetLife" or the "Company"). Customers, employees, and business partners around the world provide the Company with personal information and other confidential information every day in order to conduct its global operations. MetLife is firmly committed to the protection of the confidential information of the Company and its customers, employees and business partners, as well as the responsible use of personal information, respecting individual's privacy rights, and processing personal information in compliance with applicable laws and regulations.

This document describes key aspects of MetLife's Global Privacy & Information Security Program (the "Program"). The objectives of the Program are to:

- Protect the privacy and security of individuals' personal information and our customer's confidential information by adopting and implementing administrative, technical, including cybersecurity controls and physical, safeguards;
- Protect against known and unknown threats or hazards to the availability, confidentiality, and integrity of personal information and other confidential information; and,
- Protect against loss or destruction or unauthorized access to personal information and other confidential information.

The Program is shared by the Privacy Compliance Group ("PCG") and Information Security Office ("InfoSec").

MetLife's Privacy Compliance Group

MetLife's Privacy Compliance Group ("PCG") has oversight of MetLife's Privacy Compliance Program and is responsible for establishing and maintaining the internal Global Privacy and Data Protection Policy ("Global Privacy Policy"), overseeing the implementation of and ongoing compliance with the Global Privacy Policy and advising business management on privacy risks. The Global Privacy Policy establishes enterprise-wide principles and global minimum standards designated to facilitate compliance with applicable privacy laws and regulations in the countries in which MetLife conducts business.

The PCG tracks privacy and data protection trends, developments and emerging risks in part through active membership and participation in professional organizations, and employs a highly skilled staff of privacy professionals, a majority of whom hold one or more industry-recognized designations from the International Association of Privacy Professionals ("IAPP") and attend professional conferences and training to stay abreast of emerging privacy and data protection developments. The authority and responsibility for managing the Privacy Compliance Program resides with MetLife's Chief Privacy Officer ("CPO"). The CPO is a senior-level executive responsible for establishing and maintaining the vision, strategy and Program. The CPO is supported by the PCG, including appointed regional privacy leads.

The PCG works in partnership with our locally appointed Data Protection Officers ("DPOs"), who are consulted on issues of data protection and privacy matters related to the processing of personal information.

Information Security

The mission of InfoSec's program is to protect MetLife's information and technology assets, personal and confidential information, and technology dependent business processes from known and unknown risks and security threats, and to provide enterprise-wide IT risk identification, prioritization, reporting, and mitigation services. InfoSec pursues this mission through the establishment of programs to protect against, monitor and/or report threats to MetLife's information and technology assets, associated with the risks of operational disruption and unauthorized or accidental access, modification, destruction, exposure and/or disclosure. This program is centered on fostering and raising awareness on appropriate IT and physical security practices, along with establishing integration points with business process operations to protect MetLife data.

The authority and responsibility for managing the InfoSec program resides with MetLife's Enterprise Chief Information Security Officer ("CISO"). The Enterprise CISO is a senior-level executive responsible for establishing and maintaining the vision, strategy and program so that information and technology assets are protected among all MetLife affiliates and that IT risks are reported, remediated and managed.

Administrative Safeguards

MetLife's Program includes a set of written policies, standards and procedures, available to MetLife employees via our intranet policy system.

Certain policies and standards are established at the corporate level and apply generally to all MetLife affiliates and businesses. Each of MetLife's affiliates and businesses may adopt supplementary policies and standards as appropriate to reflect the circumstances of their own operations. PCG reviews those policies and standards for consistency with MetLife enterprise policies and standards.

MetLife's Global Privacy and Data Protection Policy

MetLife's Global Privacy and Data Protection Policy includes the following standards based on its key principles:

(i) Provide individuals notice about the use and purpose for processing personal information;
(ii) Limit the amount of personal information collected and processed;
(iii) Conduct due diligence and ongoing monitoring of the Company's third parties;
(iv) Ensure that the cross-border transfer of personal information is compliant with governing laws and regulations;
(v) Incorporate end-to-end privacy in the development of technologies and business solutions, and
(vi) Implement safeguards and report events impacting the availability, confidentiality and integrity of personal information.

Global and Local Privacy Policies and Procedures

MetLife and its employees are subject to, and must comply with, the applicable privacy laws of the jurisdictions in which MetLife conducts business. If the privacy laws or regulations in a country where MetLife operates establish requirements that are higher than those established under the Global Privacy Policy, employees in that country follow those requirements through local policies, standards and procedures

Privacy Risk Analysis

The MetLife Privacy Risk Analysis ("PRA") (commonly referred to as a "privacy impact assessment") process is an essential component of the MetLife Privacy Compliance Program to help establish proactive privacy protection measures. MetLife's PRA process allows for the identification and resolution of potential privacy deficiencies at an early stage of projects, products or technologies processing personal information.

MetLife's Code of Business Ethics & MetLife Policies

MetLife's Code of Business Ethics (the "Code") requires employees to protect personal information. MetLife's Code, together with MetLife's policies, gives employees information they need to perform their jobs ethically and in line with MetLife's standards and applicable laws and regulations. Employees are responsible to protect and limit their use of personal information and respect the privacy of MetLife employees, customers, business partners and all other individuals whose personal information MetLife processes.

Email

Disclosure of confidential and personal information about MetLife operations, employees, services or systems to any recipient not authorized to receive such information is prohibited.

MetLife’s IT Security Policies include guidance on the use of communication resources, cryptographic controls, exchange agreements with other organizations and methods to protect sensitive data sent external to MetLife including use of TLS and Send Secure to encrypt the confidential information. Encryption is designed to prevent the information from being read or corrupted as it travels from MetLife, over the Internet, to the recipient’s mailbox.

Software

Software developed at MetLife is the property of MetLife. Data in MetLife custody is treated in a proprietary and confidential manner. It is used for company business, and not disclosed to third parties outside of MetLife without proper authorization. Decisions to upgrade to a new release of software take into account the security of the release (i.e., the number and severity of security vulnerabilities affecting the version). Such upgrades are conducted in accordance with MetLife's IT Security Policy Change Management requirements.

Devices Equipped with Photographic, Audio or Video Recording and/or Transmission Capabilities

Use of photographic, audio and video recording devices in the workplace is governed by a policy that states employees may not use recording or transmitting devices to record or retransmit any MetLife documents or confidential or personal information, except for MetLife business purposes consistent with MetLife policies and practices.

Privacy and Information Security Training and Awareness

MetLife written policies are reinforced by communications and training programs, instructing employees to treat nonpublic business and personal information as confidential and subjecting employees to disciplinary action if they fail to do so.

MetLife communicates to our employees concerning MetLife standards that relate to confidentiality and the protection of personal information. In addition, where indicated by the Company’s guidelines, MetLife requires third parties to whom personal information is communicated in the course of business dealings to safeguard that information from improper disclosure.

MetLife Privacy and InfoSec Policies are published on the intranet and accessible to MetLife employees. Formal Policy Lifecycle Management disciplines are in place to govern aspects of intake (i.e., proposed changes to existing policies and standards), impact analysis, change management, approvals, voting and communication. Policy Voting and Policy Communication committees regularly convene to support such activities.

MetLife has mandatory online training programs for MetLife employees, including but not limited to privacy, code of business ethics and InfoSec. The courses are regularly updated and have been designed to complement and reinforce MetLife policy and culture around the confidentiality of personal and confidential information. Upon being hired, new employees are required to complete such mandatory trainings so that employees understand expected behaviors, in compliance with applicable policies, laws, and regulations. MetLife continues to provide ongoing training and updates to employees on emerging issues, information and best practices. Policies and training topics include but are not limited to:

- Share only on a “need to know” basis. Personal and confidential information should be accessed, used and disclosed by employees, and others who are MetLife service providers, only on a business “need to know” basis and with the proper management approvals;
- Secure desks and/or offices, including home offices. Secure any confidential information when employees leave their desk or leave for the day; and,
- For remote employees, connect to the MetLife’s Virtual Private Network (VPN), utilize only trusted networks, and abide by MetLife’s privacy principles.

MetLife regularly communicates to employees about emerging risks, policy requirements, and the importance o and protecting company and personal information through email reminders, intranet posts, ad-hoc trainings, and internal social channels sponsored by the PCG and InfoSec.

Information Lifecycle Management ("ILM") Program

Information is a corporate asset, and its proper management enables MetLife to improve operational efficiency and customer satisfaction, make more informed business decisions, and remain in compliance with laws and regulations.

MetLife has a global corporate ILM program that manages all its information no matter how it is created or where it is located or stored in the Company. At MetLife, information is classified into two categories: records and non-records. The ILM program governs the management of MetLife information through a governance structure that:

- Provides leadership and guidance to manage information as a corporate asset;
- Ensures the lines of business, corporate functions and regions are in compliance with the ILM Policy;
- Supports the effective management of information through ILM policies, standards, processes, procedures and the record retention schedule; and,
- Monitors compliance with legal/regulatory obligations regarding the retention and disposal of records.

The ILM Program Office, in partnership with the PCG and InfoSec, works with employees to manage information strategically and holistically throughout its lifecycle including the creation, storage, usage, collaboration, preservation, archiving and disposal of MetLife information. Below are the key aspects of the ILM Program.

Ownership of Information

MetLife information is MetLife's property and does not belong to any employee or third party, unless agreed to by the employee or third party and MetLife. All employees and third parties with access to MetLife's Information, including system/applications containing MetLife information, are responsible for managing information in accordance with MetLife's ILM governance framework that includes policies, standards, processes, procedures, guidelines and the MetLife's record retention schedule. MetLife information that is created or received from third parties is managed in accordance with MetLife's ILM framework. When an employee's employment ends or the contractual relationship of a third party with access to MetLife information ceases, neither the employee nor third party shall retain or possess any MetLife information after the employment or contractual relationship ceases unless required by law. Originals and copies of MetLife information in the possession of the employee or third party, must be returned to MetLife or be destroyed.

MetLife Record Retention Schedule

MetLife's Global Record Retention Schedule ("Schedule") establishes the requirements for retaining and disposing of corporate records in compliance with legal and regulatory requirements, as well as MetLife business needs. The ILM Program Office conducts an annual recertification of the Schedule so that it aligns with business needs as well as legal and regulatory requirements. MetLife records are retained until the retention requirement stated in the Schedule has been met. Non-records have a maximum retention period of six years but may be disposed of at any time prior to six years when no longer needed.

Disposal of Information

Once the record retention requirement has been met, MetLife's ILM policy requires information to be securely disposed of when no longer required to meet business or regulatory obligations, absent a legal hold or preservation obligation in place.

Records Management Vendors

MetLife has records management vendors that provide secure services for storage, retrieval, and disposal of paper and electronic records once the records have met their retention requirements, unless there is a preservation obligation or legal hold in place.

All Shred Program and Clean Desk Guidelines

MetLife U.S. operations follow an “All Shred Program,” in which secure shred bins or consoles are used to securely dispose of information on paper that has met its retention or is no longer needed for business purposes, absent a legal hold or other preservation obligation, mandating their further preservation. Globally, employees are required to comply with MetLife Clean Desk guidelines to help MetLife reduce the risk of information theft, fraud, or a security breach caused by sensitive information being left unattended.

ILM Training Course

MetLife’s ILM mandatory training course is provided to employees. The course helps employees better understand how to manage information through its lifecycle and the role of the Information Lifecycle Management Program in ensuring employees and our business partners retain the right information, for the right time and the right purpose.

Call Center Procedures

MetLife’s call center consultants follow documented procedures to authenticate callers before disclosing any confidential information about individuals. Before disclosing any information about policy owners, insured individuals, claimants, beneficiaries or others, consultants follow authentication procedures to verify a caller’s identity.

Technical and Cybersecurity Safeguards

MetLife reviews and updates policies and procedures to keep them current in light of evolving cybersecurity law and regulation, emerging threats and new and changing technologies. InfoSec works with IT and business management to institute controls for IT systems, applications and databases, and for vendor and application service provider arrangements.

MetLife's approach to securing our environment is based on the National Institute of Standards and Technology ("NIST") Cybersecurity Framework ("CSF"). The CSF is based on existing standards, guidelines, and practices for MetLife to better manage and reduce cybersecurity risk. The core high level functions of the framework are Identify, Protect, Detect, Respond and Recover. InfoSec controls, products and initiatives align to these core functions.

As a component of the CSF "Prevent" function, MetLife utilizes a three-tier approach to data protection. Our Demilitarized Zone ("DMZ") is the presentation tier. This is where our Internet-facing servers reside. It provides an area where MetLife can place its content servers for access by the Company's customers and creates an area that, if compromised, would limit the exposure to MetLife data. Under normal conditions, traffic is limited from the Internet to the DMZ only. Our second tier, known as the Bastion, is the application tier. The Internet application servers reside in this area and can communicate, on a limited basis, with both the DMZ and our internal network. The third tier, the data tier, resides inside the MetLife internal network. Application and database servers and business logic are in the Bastion behind both sets of firewalls. MetLife uses redundant firewalls in the DMZ and redundant firewalls in the Bastion. InfoSec employs security scans to monitor for policy noncompliance and vulnerabilities at various levels of the technology infrastructure, as well as on various applications. Performance measures for key security processes critical to the security of the IT environment (e.g., anti-malware reports and spam totals) have been defined and aligned to the CSF "Detect" function. InfoSec has oversight responsibilities over these processes through IT internal risk reporting.

As a component of the CSF "Respond" function, MetLife has a Cyber Security Incident Response Team ("CSIRT") that is charged with responding to internal and external threats and taking action. The CSIRT is responsible for establishing and maintaining visibility and situational awareness of threats, vulnerabilities and incidents. The team implements proactive measures in response to changes in the threat environment and works to rapidly contain security incidents. The primary goals of the CSIRT are to rapidly detect, triage, contain, eradicate and recover from computer security incidents, working closely with other teams across MetLife throughout the incident lifecycle. The team is staffed with dedicated incident responders and forensics investigators and manages multiple third party contracts to assist MetLife with its response anywhere it operates.

PCI DSS Requirements

The Payment Card Industry Data Security Standard (PCI DSS) is a set of global standards designed for companies that process, store, or transmit payment card information to maintain secure environments that protect cardholder data. The Payment Card Industry was founded by five of the major credit card brands, Visa, MasterCard, Discover, American Express and JCB, who also enforce the requirements.

MetLife and its affiliates accept credit and debit cards as payment for some of their products and services using the brands' networks, and, to that extent, they comply with the PCI DSS.

Technical Controls

MetLife implements the following technical controls that align to protect against threats and unauthorized access.

Access Security, Recertification and Removal

Electronic records are protected through the use of multiple computer software products that employ such security features as passwords, user identification and personal identification numbers to guard against unauthorized access. Based on risk, MetLife IT systems, applications and databases must periodically undergo employee access recertification. Managers must recertify that it is appropriate for employees to continue to have access to these systems, applications, and databases. In addition, the recertification process is in place at the platform level for when employees change job responsibilities. Access of any departing employee to our platforms is removed as soon as the departure is processed through Human Resources.

Anti-Malware Software; Standard Configuration; Backups

Electronic points of entry, as well as servers, email, and workstations, are protected by anti-malware software. MetLife follows industry best practices for configuration of initial builds and vulnerability management to integrate security controls.

Anti-Phishing/Anti-Fraud

MetLife utilizes a vendor that actively scans the web for sites that may be masquerading as legitimate MetLife websites. The intent of this scanning is to identify websites that could obtain confidential information from MetLife customers who believe that they are interacting with the MetLife site. This vendor seeks out potential fraudulent activity and notifies MetLife upon any discoveries. It also can assist MetLife in shutting down these offending sites. MetLife also partners with an industry-leading vendor for frequent phishing exercises to test employee awareness.

Application Testing

MetLife leverages independent application vulnerability scans and ethical hacks to test the controls implemented to protect the confidential and personal information.

Business Continuity/Disaster Recovery/Cyber Resiliency

To minimize potential losses and to permit resumption of processing in line with business recovery objectives, there are centrally coordinated business continuity and disaster recovery plans for MetLife systems and data consistent with the impact of any system failures on the business. These plans include a suitable backup and disaster recovery plan that is maintained, properly documented, periodically tested, and appropriate for the system covered, and each includes exercises in crisis management, IT recovery, business resumption, and security incident management.

MetLife’s backup strategy has been engineered to maximize the ability to recover in a timely manner while protecting personal information. MetLife core systems are replicated from primary data centers to our secondary data centers. In addition, MetLife keeps an enterprise grade backup strategy in alignment with best industry practices to further ensure systems resiliency and capacity to recover from emergency situations with minimum impacts.

Data Protection

MetLife employs an enterprise-wide data loss protection infrastructure at the network perimeter and workstation level, which monitors for and alerts MetLife about confidential data being moved from MetLife over the Internet or via insecure channels including web uploads, removable devices, physical printing, and email.

Encryption

MetLife encrypts data at rest on personal computers, including both laptops and desktops, mobile devices, and servers. Mobile phones are managed by a mobile device management solution that encrypts the device. Email

Encryption is enforced centrally using Transport Layer Security TLS or our encrypted messages Internet facility via our "Send Secure" email function. External websites leverage up-to-date secure versions of TLS.

Two-Factor Authentication

MetLife strictly controls remote access to its networks through two-factor authentication. Through the use of hard and soft tokens, MetLife can control access to MetLife systems for any employees who require access to MetLife networks while out of the office.

Vulnerability Management

MetLife utilizes a number of vulnerability management tools to filter and risk rank security alerts that are received daily; assisting in distinguishing between alerts relevant to MetLife versus alerts that have no bearing on MetLife's infrastructure, allowing MetLife to focus on the most significant threats.

Risk Assessment

MetLife has developed an IT risk management framework to assess MetLife's information technology risks. This program includes assessment of risks for MetLife's IT organizations and technology infrastructure. The goals of the risk assessment process include prioritization of identified risks, and evaluation by IT management as to whether risks are being appropriately managed.

MetLife also assesses the sufficiency of IT policies, standards, procedures, information systems and other arrangements in place to control risks. MetLife reviews these policies, standards, procedures and other arrangements on an ongoing basis and updates them whenever as warranted. MetLife employees can submit a change request for review by the policy owner and approval processes are in the IT Security policies system.

Monitoring, Testing, and Auditing

MetLife monitors the effectiveness of its information security practices. Business applications that are either new or undergoing major enhancements are evaluated through an internal application assessments process. New applications and major changes to existing applications go through the phased gate review process, which requires key project stakeholders and senior management approval at primary project milestones from deployment to production. Servers are scanned regularly so that they meet the current security standards.

MetLife works with leading third party security companies who help periodically assess prevalent threats and vulnerabilities to enhance our security program. These services include periodic penetration testing and review.

MetLife employs network surveillance software to determine if any abnormal activity occurs, such as an attempt to gain unauthorized access to MetLife's internal systems from outside MetLife's network. Incidents are escalated to MetLife executive management in accordance with incident handling procedures. On top of internal measures, all Intrusion Detection System ("IDS") components are centrally monitored by a managed security services supplier 24 hours a day, seven days a week. If any suspicious or abnormal network traffic occurs, appropriate IT security personnel are alerted.

Additionally, MetLife's Internal Audit organization conducts periodic audits for the security and confidentiality of MetLife and MetLife's personal information.

Physical Safeguards

MetLife facilities, including offices and data centers, have physical security controls in place designed to prevent unauthorized access.

MetLife's facilities dedicated to computer processing are physically restricted and access is only granted to persons who have legitimate business responsibilities in the facility. MetLife buildings that house critical IT facilities use electronic and mechanical locks, employ trained security guards, use pictured badges for individual display and are applied for electronic access controls, and operate video surveillance to protect against unauthorized physical access. Any potential incidents of unauthorized access are required to be reported immediately to the site security management for immediate action.

Personal Data Incident Handling

MetLife maintains policies and procedures outlining what employees and business units must do if a Personal Data Incident occurs. MetLife's data incident management procedures establish a framework to facilitate a coordinated, efficient response across the enterprise.

When a Personal Data Incident ("PDI") is reported, the PDI is analyzed by the PCG and DPOs, together with MetLife's Legal Department. The definition of data breach varies from country to country, as do the reporting obligations to the authorities and notification requirements of the affected individuals. If notification to impacted individuals or regulators is required or desired, the PCG, Compliance Department, and DPO, as appropriate, work with the business to notify and, as appropriate, provide credit monitoring.

The incident response process is designed so that (i) the appropriate MetLife individuals are alerted, (ii) the Personal Data Incident is appropriately assessed, managed, contained, and remediated, and (iii) root cause, lessons learned, and remediation activities are appropriately reviewed and addressed to prevent future incidents.

Employees receive training on how to identify, report and prevent PDI's from occurring.

Third Party Service Providers

MetLife exercises due diligence in selecting its service providers, including review of vendor applications, general IT controls and the IT facilities used to service MetLife's business.

MetLife's Corporate Functions ("CFs") and Lines of Business ("LOBs") are responsible for ensuring that engagements with third party suppliers comply with the requirements set forth in the Global Sourcing and Third Party Risk Management Policy ("TPRM Policy"). Service providers acting on behalf of MetLife are obligated to protect the security and confidentiality of MetLife's systems and information.

When selecting service providers who may have access to confidential and personal information, MetLife employees must exercise care and follow MetLife's TPRM Policy and procedures. Before onboarding new providers, MetLife employees query prospective service providers about their information security policies and procedures as part of their due diligence during the selection process and perform due diligence if the service provider or its personnel will have access to confidential and/or personal information. Through this process, MetLife can assess whether a potential service provider has the appropriate policies, procedures, controls and personnel to be entrusted to process such information pursuant to MetLife standards and in compliance with applicable regulatory and legal requirements.

MetLife service providers must enter into a MetLife-approved written contract that includes terms and conditions that require that MetLife and MetLife customer information be treated confidentially and used only as necessary to perform the contracted services.

In accordance with the criteria (e.g., materiality thresholds) set in the Global Sourcing & Third Party Risk Procedures for the applicable region or country, a Request for Proposal ("RFP") may be employed. Among other things, the RFP documentation alerts potential vendors that they must agree to appropriately ensure the security and confidentiality of MetLife data and personal information, and that this applies similarly to any person or entity with whom they share such information. A MetLife contract form containing appropriate provisions to protect MetLife data and/or personal information typically accompanies the RFP. In addition, potential vendors are generally asked to provide references.

MetLife reviews service provider compliance with information security and privacy requirements with the service provider. Ongoing privacy monitoring is conducted through privacy risk assessments. InfoSec reviews controls to make sure that any MetLife data and/or personal information planned to be resident and processed at the vendor's site will be secured and protected from unauthorized use or disclosure.

Through the MetLife Third Party Risk Assessment process, service vendors must periodically update the assessment documentation and be reevaluated relative to their internal controls.

Non-Domestic Service Providers

As a result of its ongoing risk assessment, MetLife developed a set of guidelines that detail the special arrangements MetLife expects for non-domestic providers.

MetLife business management must be informed of any offshore arrangements when their applications and data fall within the scope of that arrangement.

For non-domestic service providers, MetLife's requirements include:

- A Third Party Risk Assessment;
- Cross-border data transfer mechanisms where legally required, or as appropriate;
- To the extent consistent with local law, the service provider must perform a background check on personnel providing services to MetLife;
- Access to MetLife systems and data must be granted, reviewed and removed in accordance with MetLife's IT standards;
- Provide security and privacy awareness training to personnel working on MetLife projects; and,
- Provide MetLife with the steps they have taken to assure that MetLife's information is treated confidentially, and that the information is accessed on a need-to-know basis. The description must outline:
  - Physical safeguards of MetLife data (e.g., separate workspaces, locking cabinets, building security).
  - Technical safeguards (e.g., encryption, two-factor authentication).
  - Administrative safeguards (e.g., log review, documented procedures, audits).

The contractual requirements outlined within the scope of the relationship apply not only to any agreements between the service provider and MetLife, but also between the service providers and any of its subcontractors hired for MetLife-related work.

Post Pandemic and Future Work Arrangements

MetLife is committed to protecting and elevating the security of personal information even in times of crisis. During this time, MetLife has increased scrutiny on third party due diligence, conducted internal privacy assessments for new tools and novel uses of data, enhanced Data Loss Prevention ("DLP") practices and arranged secure remote work capabilities for employees.

In further support of our commitment to privacy and data protection, MetLife has communicated the activities above across the enterprise and engaged in a number of awareness campaigns so that MetLife's privacy expectations are met while employees work remotely. These efforts include, but are not limited to:

- Video-training materials;
- Privacy presentations and panels with guest speakers;
- Intranet postings promoted by PCG, InfoSec, risk partners and others; and,
- Cross-functional recurrent local, regional and corporate privacy meetings.