

個人情報保護方針(プライバシー・ポリシー)

ミュンヘン再保険会社 日本支店(以下「当支店」といいます)は、個人情報保護の重要性に鑑み、個人情報保護法等の関係法令等を遵守し、この個人情報保護方針(以下「この方針」といいます)に則って、個人情報を適正に取扱うとともに、個人情報保護にかかる安全管理について適切な措置を講じます。また、当支店は、個人情報の取扱いが適正に行われるように従業員教育・指導を徹底します。さらに、当支店はこの方針について、適宜見直し改善いたします。

なお、個人番号をその内容に含む個人情報は、法令により利用目的が制限されているなどの点でそれ以外の個人情報と異なるため、この方針の対象外としますが、別途法令に則り適切に取得、利用、保管、廃棄等いたします。

当支店のウェブサイトは、ミュンヘン再保険会社(ドイツ)が運営しています。そのため、クッキーの使用に関する情報は、関連するデータ保護宣言に記載されていますので、下記リンク先をご覧ください。

<https://www.munichre.com/en/general/privacy.html>

1. 当支店の名称、住所および代表者の氏名

ミュンヘン再保険会社 日本支店

〒100-6113 東京都千代田区永田町 2-11-1 山王パークタワー13 階

日本における代表者、CEO 秦泉寺 大興

2. 個人情報の取得

当支店は、業務上必要な範囲内で、かつ適法で公正な手段により個人情報を取得します。

3. 個人情報の利用目的

当支店は、下記の目的に必要な範囲内で個人情報を利用します。また、利用目的を変更する場合には、その内容をご本人に通知するか、ホームページ等に公表します。

- (1) 再保険契約のリスク分析、引受、履行および管理
- (2) 再保険金、給付金等の支払い査定および支払い
- (3) 再々保険契約の締結
- (4) 顧客企業等に対する各種情報の提供ならびにセミナーおよびマーケットイベント開催のご案内
- (5) 顧客企業等に対する顧客満足度調査等の各種アンケートの実施
- (6) 顧客企業等に対する保険契約データ等のデータ分析およびコンサルティングサービスの提供
- (7) 当支店従業員等の採用および人事管理
- (8) その他、上記(1)から(7)に関連または付随する業務

4. 個人データの安全管理

当支店は、個人データの漏えい、滅失または毀損の防止その他、個人データの安全管理のため、取扱規程等の整備、アクセス管理、その他安全管理措置に係る実施体制の整備等、十分なセキュリティ対策を講じます。また、当支店が、利用目的の達成に必要な範囲内において外部に個人データの取扱いを委託する場合には、委託先の選定基準を定め、あらかじめ委託先の情報管理体制を確認し、委託後の業務遂行状況を監視するなど、委託先に対する必要かつ適切な監督を行います。その主な内容は下記のとおりです。

(1) 個人情報保護方針(プライバシー・ポリシー)の策定

個人データの適正な取扱いの確保のため、「関係法令・ガイドライン等の遵守」、「質問および苦情処理の窓口」等について個人情報保護方針(プライバシー・ポリシー)を策定しています。

(2) 個人データの取扱いに係る規律の整備

個人データの取得、利用、移送、消去等の段階ごとに取扱方法を定めた「個人情報保護規程」を策定しています。

(3) 組織的安全管理措置

個人データの取扱いに関する総括責任者および部管理責任者を設置するとともに、個人データを取り扱う従業員および当該従業員が取り扱う個人データの範囲を明確化し、個人情報保護法や個人情報保護規程に違反している事実または兆候を把握した場合の報告体制を整備しています。また、個人データの取扱状況について、定期的に自己点検を実施するとともに、コンプライアンス・オフィサーによるレビューを実施しています。

(4) 人的安全管理措置

個人データの取扱いに関する留意事項について、従業員に定期的な研修を実施しています。また、個人データについての秘密保持に関する事項を就業規則に記載しています。

(5) 物理的安全管理措置

当支店のオフィスにおいては、入退室管理を実施するとともに、個人データの取扱いを含む執務は従業員等のみが入室できる区域でのみ行っています。また、個人データを保存する当支店のサーバーは施錠できる部屋に設置し、その部屋への立入りは権限を付与した従業員等に限定しています。

(6) 技術的安全管理措置

担当者の業務に応じて、アクセス権が適切な範囲に限定して付与されるよう、アクセス制御を実施しています。また、個人データを取り扱う情報システムを外部からの不正アクセスから保護する仕組みを導入しています。

(7) 外的環境の把握

当支店が外国の第三者に個人データを提供する場合は、当該外国における個人情報の保護に関する制度の有無や、当該外国の個人情報の保護に関する制度についての指標となり得る情報の存在(例: 当該外国が GDPR 第 45 条に基づく十分性認定の取得国であることや APEC の CBPR システムの加盟国であること)を把握した上で、安全管理措置を実施しています。

5. 個人データの第三者への提供

当支店は、下記の場合を除いて、あらかじめご本人の同意を得ないで、個人データを第三者に提供することはいたしません。

- (1) 法令に基づく場合
- (2) 利用目的の達成に必要な範囲内においてミュンヘン再保険会社のグループ会社と個人データを共同利用する場合
- (3) 利用目的の達成に必要な範囲内において個人データを委託先に提供する場合
- (4) その他、個人情報保護法に基づき、ご本人の同意を得ないで個人データを第三者に提供することが認められている場合

当支店は、個人データの取扱いについて個人情報保護法に基づき講ずべき措置に相当する措置を継続的に講ずるために必要な基準に適合する体制を整備している外国にある第三者に対して個人データを提供することがあります。これらの措置の内容等に係る情報提供を希望される方は、下記 11. のお問い合わせ窓口までお問い合わせください。

6. 個人データの共同利用

当支店は下記のとおり、個人データをミュンヘン再保険会社のグループ会社と共同利用いたします。共同利用の対象となる個人データの管理責任者は、当支店（当支店の住所および代表者名は上記 1. 記載のとおりです）とします。

- (1) 上記 3. (1)および(2)に記載した利用目的のための共同利用

- (A) 共同利用する個人データの項目

被保険者の住所、氏名、性別、生年月日、保険金額、その他元受保険会社の申込書等に記載された内容

- (B) 共同利用するグループ会社名（所在国）

Munich Management Pte Ltd（シンガポール）

New Reinsurance Company Ltd.（スイス）

- (2) 上記 3. (4)および(5)に記載した利用目的のための共同利用

- (A) 共同利用する個人データの項目

顧客企業等の担当者等の氏名、所属部署、肩書

- (B) 共同利用するグループ会社名（所在国）

Munich Management Pte Ltd（シンガポール）

New Reinsurance Company Ltd.（スイス）

7. 個人データの委託

当支店は、再保険料や再保険金の計算等の事務処理のため、個人データを外部に委託する場合があります。

また、従業員の給与支払関連事務(税金、年金を含む)を、外部の人事サービス専門業者に委託しております。

8. 保有個人データの開示、訂正・削除等または利用停止等

本人自身に関する保有個人データの開示または利用目的の通知のご依頼があった場合は、請求者がご本人であることを確認した上で、法令に従い、その内容を回答いたします。

開示は、原則としてご請求者が請求した方法により行います。ただし、当該方法による開示に多額の費用を要する場合その他当該方法による開示が困難である場合は、開示は書面により行います。

また、訂正・削除等または利用停止等のご依頼があった場合には、必要な調査を行ったうえで法令に従い適切な対応を行うほか、実務的に可能な範囲で自主的に利用停止等に応ずることといたします。

開示、訂正・削除等または利用停止等のご依頼があった保有個人データが元受保険会社から取得されたものであった場合は、必要に応じて当該元受保険会社と協議した上で、適切に対応いたします。

これらのご依頼は、下記 11. お問い合わせ窓口まで、郵送にてお願いいたします。この際、ご請求者の本人確認のために、以下の書類についてもあわせてご送付願います。請求書類等の送付に係る費用についてはご請求者のご負担となりますのでご了承ください。

(1) ご請求者がご本人の場合

下記(A)および(B)の書類

(A) 下記(i)から(vi)のいずれかの書類の写し

- (i) 運転免許証
- (ii) 健康保険証
- (iii) パスポート
- (iv) 個人番号カード(おもて面)
- (v) 在留カード
- (vi) 特別永住者証明書

(B) 現住所が記載され、発行日から3か月以内の住民票の写し。住民票の写しは、地方公共団体が発行する公文書をご送付いただくこととし、その複写物は認められません。住民票の写しに個人番号の記載がある場合は、個人番号を黒塗りしてください。

(2) ご請求者が代理人の場合

下記(A)から(D)の書類すべて

- (A) 上記(1)の本人確認書類
- (B) 当該代理人の本人確認書類(書類の種類は上記(1)と同様です)
- (C) 法定代理人の場合は法定代理権があることを確認できる書類(戸籍謄本、成年後見登記事項証明書等。発行日から3か月以内のもの。)
- (D) 委任による代理人の場合は委任状(委任者であるご本人の実印押印のもの)および発行日から3か月以内のご本人の印鑑証明書

9. 第三者提供記録の開示

上記 8. 保有個人データの開示、訂正・削除等または利用停止等は、当該本人が識別される個人データに係る第三者提供記録の開示請求について準用します。

10. 匿名加工情報の取扱いについて

(1) 匿名加工情報の作成

当支店は、匿名加工情報の作成はいたしません。

(2) 匿名加工情報の提供

当支店は、匿名加工情報を第三者に提供する場合には、提供しようとする匿名加工情報に含まれる個人に関する情報の項目と提供の方法を公表するとともに、提供先となる第三者に対して、提供する情報が匿名加工情報であることを明示します。

(3) 匿名加工情報に関する公表

当支店が保有する匿名加工情報について、当該情報が匿名加工情報であることを明示したうえで、継続的に第三者に提供いたします。

(A) 匿名加工情報に含まれる個人に関する情報の項目

- (i) 年齢(生年月)
- (ii) 性別
- (iii) 社会保険の資格情報(本人・家族区分、資格取得・喪失年月等)
- (iv) 診療報酬明細書の記載内容(傷病名、入退院(通院)年月日、診療年月日等)
- (v) 健診項目データ(数値等)
- (vi) 健診実施日付、保健指導項目データ(数値等)
- (vii) ライフログ情報(歩数等)

(B) 提供の方法

- (i) 電子メールによる送信
- (ii) ファイル共有サービスによる提供

11. お問い合わせ窓口

当支店は、個人情報の取扱い、安全管理に関するご質問、苦情について、適切に対応する所存ですので、下記窓口までご連絡ください。

ミュンヘン再保険会社 日本支店

〒100-6113 東京都千代田区永田町 2-11-1 山王パークタワー13 階

Tel: (03) 5251-6862(コンプライアンス・オフィサー)

(受付時間:9 時～12 時および 13 時～17 時、土日祝祭日および 12 月 31 日から 1 月 3 日までを除く)

12. 認定個人情報保護団体および苦情の解決の申出先

当支店は、認定個人情報保護団体である一般社団法人外国損害保険協会の対象事業者です。

ホームページ: <https://www.fnlia.gr.jp/>

＜当支店の契約する指定紛争解決機関について＞

当支店は、法律に定められた指定紛争解決機関である一般社団法人保険オンブズマンと手続実施基本契約を締結しています。当支店との間で問題を解決できない場合には、解決の申立てを行うことができます。

詳細は下記ホームページをご覧ください。

一般社団法人保険オンブズマン

Tel: 03-5425-7963

(受付時間:9 時～12 時および 13 時～17 時、土日、休日、年末年始等を除く)

ホームページ: <https://www.hoken-ombs.or.jp/>

Privacy Policy

Munich Re, Japan Branch (hereinafter the “Branch”), understanding the importance of protection of personal information, shall comply with any law and regulation such Act on the Protection of Personal Information, including this privacy policy (hereinafter the “Policy”), relating to the protection of personal information, and shall handle personal information properly and implement appropriate security measures for the protection of personal information. In addition, the Branch shall educate and direct its employees in order to enable them to handle personal information appropriately. The Branch shall review and adjust the Policy as it becomes necessary.

The personal information that includes Individual Number is different in its nature from other personal information, e.g. its purpose of utilization is restricted under the relevant laws and regulations, and thus it is out of the scope of this Policy. Nevertheless, the Branch shall acquire, utilize, retain and dispose it appropriately in accordance with such relevant laws and regulations.

The Branch’s website is operated by Munich Reinsurance Company (Germany). You will therefore find information on the use of cookies in the relevant data protection declaration. Please click here <https://www.munichre.com/en/general/privacy.html>

1. Name and Address of the Branch and Name of the Representative

Munich Re, Japan Branch
Sanno Park Tower 13F
2-11-1 Nagatacho, Chiyoda-ku, Tokyo 100-6113

Brian Jinzenji (Representative for Japan, CEO)

2. Acquisition of Personal Information

The Branch shall acquire personal information, as long as it is necessary for the conduct of its business, by lawful and fair measure.

3. Utilization Purpose of Personal Information

The Branch shall utilize personal information as long as it is necessary to achieve the purposes listed below (hereinafter the “Utilization Purpose”). If the Branch changes the Utilization Purpose, it shall notify the principal of the change, or announce the change publicly on its homepage, etc.

- (1) Risk assessment, acquisition, maintenance and management of reinsurance;
- (2) Assessment and payment of reinsurance benefits etc.;
- (3) Conclusion of retrocession agreements;
- (4) Provision of various information and introduction of seminars and market events to business partners;

- (5) Taking various surveys from business partners such as customer satisfaction surveys;
- (6) Data analysis of insurance policy data and provision of consulting services to business partners
- (7) Recruiting and personnel management of employees of the Branch; or
- (8) Any other purposes of personal information utilization incidental or relating to (1) to (7) above.

4. Security Measures for Personal Data

In order to protect personal data, including but not limited to, to prevent leakage, disappearance or impairment of personal data, the Branch shall implement sufficient security measures, such as the creation of internal regulations on how to handle personal data, and access management.

When the Branch outsources the handling of personal data to a third party in order to achieve the Utilization Purpose, the Branch shall conduct necessary and appropriate supervision on the third party, including but not limited to, setting a criterion of outsourcee, reviewing data security measures implemented at the outsourcee's premises before outsourcing the personal data, and monitoring how the outsourcee handles the outsourced data. The main contents are as follows:

(1) Establishment of the Privacy Policy

In order to ensure the proper handling of personal data, the Branch has established the Privacy Policy regarding "compliance with related laws, regulations, guidelines" and "contact points for questions and complaints", etc.

(2) Maintenance of rules for the handling of personal data

The Branch has established "Personal Information Protection Regulations" that stipulate how to handle personal data at each stage of its acquisition, utilization, transfer, and deletion.

(3) Organisational security measures

In addition to appointing a Chief Data Manager and Departmental Data Managers for the handling of personal data, the Branch has clarified the employees who handle personal data and the scope of personal data handled by such employees, and has established a reporting system in the event that facts or signs of violations of the Act on the Protection of Personal Information or Personal Information Protection Regulations are identified. In addition, the Branch conducts periodic self-checks of the status of personal data handling, as well as reviews by the Compliance Officer.

(3) Human security measures

The Branch provides regular training to the employees on precautions regarding the handling of personal data. In addition, matters regarding the confidentiality of personal data are included in the Rules of Employment.

(4) Physical security measures

In the office of the Branch, access control is implemented, and work, including the handling of personal data, is conducted only in areas that can be accessed only by employees. In addition,

the server of the Branch where personal data is stored is installed in a lockable room, and access to the room is limited to authorized employees.

(5) Technical security measures

Access control is implemented to ensure that access rights are granted only to an appropriate extent according to the duties of the person in charge. The Branch also implemented a system to protect information systems that handle personal data from unauthorized access from outside.

(6) Understanding of external environment

In the event that the Branch provides personal data to a third party in a foreign country, the Branch implements security measures after ascertaining the existence of a system for the protection of personal information in the foreign country and the existence of information that may serve as an indicator regarding the system for the protection of personal information in the foreign country (e.g. the foreign country has obtained the adequacy decision in accordance with Article 45 of the GDPR or is a member of the CBPR system of APEC).

5. Third Party Provision of Personal Data

The Branch shall not provide any personal data to third parties without obtaining in advance a principal's consent except for following cases:

- (1) Cases based on laws and regulations;
- (2) The Branch jointly utilizes personal data with the group companies of Munich Reinsurance Company in order to achieve the Utilization Purpose;
- (3) The Branch provides personal data to an outsourcee in order to achieve the Utilization Purpose;
or
- (4) Any other cases that the provision of personal data without obtaining a principal's consent is permitted according to the Act on the Protection of Personal Information.

The Branch may provide personal data to a third party located in a foreign country that has established a system that meets the standards necessary to continuously take measures equivalent to the measures to be taken under the Act on the Protection of Personal Information with respect to the handling of personal data. If you wish to receive information regarding the details of these measures, please contact the contact point in 11. below.

6. Joint Utilization of Personal Data

The Branch may jointly utilize the personal data with the group companies of Munich Reinsurance Company as follows. The Branch is responsible for such joint utilization (the address and name of the representative of the Branch are as stated in 1. above).

- (1) Joint utilization for the Utilization Purpose written in 3.(1) and (2) above

(A) Personal data for joint utilization

Insured's name, address, gender, date of birth, sum insured, and other information included in the application, etc. submitted to a direct insurer.

(B) Names of the group companies jointly utilizing (country of the location)

Munich Management Pte Ltd (Singapore)

New Reinsurance Company Ltd. (Switzerland)

(2) Joint utilization for the Utilization Purpose written in 3.(4) and (5) above

(A) Personal data for joint utilization

Name, department and title of the personnel, etc. of the business partners, etc.

(B) Names of the group companies jointly utilizing (country of the location)

Munich Management Pte Ltd (Singapore)

New Reinsurance Company Ltd. (Switzerland)

7. Outsourcing of Personal Data

The Branch may outsource personal data to third party companies, for the performance of reinsurance administration, such as reinsurance premium calculation, sum at risk calculation, etc.

In addition, the Branch outsources its employees' payroll management and related matters (tax, pension) to a professional HR service provider.

8. Disclosure, Rectification/Deletion and Cessation of Utilization of Retained Personal Data

When an individual requests the disclosure of the Branch's retained personal data or the Utilization Purpose of such retained personal data, the Branch shall first confirm that the person requesting such disclosure is the principal. If the identity of the person is confirmed, the Branch shall disclose the retained personal data in accordance with laws and regulations.

In principle, disclosure will be made by the method requested by the requestor. However, if disclosure by this method requires a large amount of money or if disclosure by this method is difficult, disclosure will be made in writing.

When an individual requests a rectification/deletion or cessation of utilization, etc. of the retained personal data, the Branch shall conduct necessary investigation and act appropriately in accordance with laws and regulations. In addition, the Branch shall voluntarily accept the request of cessation of utilization, whenever it is practicably possible.

When the retained personal data requested for disclosure, rectification/deletion or cessation of utilization, etc. was provided by an insurance company, the Branch shall consult with the insurance company when necessary and take appropriate actions.

Any individual who requires the disclosure, rectification/deletion or cessation of utilization, etc. of personal data, is requested to contact the Branch as stipulated in below 11. by postal mail. In this case, please also send the following documents for the purpose of identification. Kindly understand that the costs for the documents shall be borne by the requester.

(1) If the individual him or herself is the requester

Both (A) and (B) below.

(A) A copy of one of (i) to (vi) below

- (i) Driver's license;
- (ii) Health insurance certificate;
- (iii) Passport;
- (iv) Individual Number card (front side);
- (v) Residence card; or
- (vi) Special permanent resident certificate

(B) A copy the certificate of residence which shows the current residence and is within 3 months from the issue date. The copy of the certificate of residence shall be the official document issued by a local public entity and its photocopy is not accepted. If the copy of the certificate of residence includes individual number, kindly mask it.

(2) If a statutory or appointed agent is the requester

All of (A) to (D) below.

- (A) Identification documents of the individual as stated in above (1)
- (B) Identification documents of the agent (the documents are same as (1))
- (C) When a statutory agent makes the request, s/he shall submit a document (which is within 3 months from the issue date) proving s/he is the statutory agent, such as an official copy of the family register or a certificate of dependent registration.
- (D) When an appointed agent makes the request, he or she shall submit a power of attorney (with the registered seal of the individual who is the madator) and the seal registration certificate of the individual which is within 3 months from the issue date.

9. Disclosure of Third Party Provision Record

The above 8. "Disclosure, Rectification/Deletion and Cessation of Utilization of Retained Personal Data" shall apply mutatis mutandis to requests for disclosure of Third Party Provision Record pertaining to personal data that identifies the individual concerned.

10. Handling of Anonymously Processed Information

(1) Production Anonymously Processed Information

The Branch will not produce Anonymously Processed Information.

(2) Provision of Anonymously Processed Information

When the Branch provides Anonymously Processed Information to a third party, the Branch shall publicly announce the items of information concerning individuals included in the Anonymously Processed Information to be provided and the method of provision, and clearly indicate to the third party that the information to be provided is Anonymously Processed Information.

(3) Public announcement on Anonymously Processed Information

With respect to Anonymously Processed Information held by the Branch, the Branch will provide such information to third parties on an ongoing basis after clearly indicating that such information is Anonymously Processed Information.

(A) Items of information concerning individuals included in the Anonymously Processed Information

- (i) Age (month of birth)
- (ii) Gender
- (iii) Social insurance eligibility information (individual/family classification, date of eligibility acquisition/loss, etc.)
- (iv) Details of the medical fee statement (name of the injury or disease, date of admission and discharge (hospital visit), date of medical treatment, etc.)
- (v) Health checkup item data (numerical values, etc.)
- (vi) Date of health checkup, data on health guidance items (numerical values, etc.)
- (vii) Lifelog information (number of steps, etc.)

(B) Method of provision

- (i) E-mail
- (ii) File sharing service

11. Contact Point

The Branch shall handle questions or complaints concerning the handling of personal information or related security measures of the Branch.

Please contact us at the number below.

Munich Re, Japan Branch

Sanno Park Tower 13F

2-11-1 Nagatacho, Chiyoda-ku, Tokyo 100-6113

Tel: 03-5251-6862 (Compliance Officer)

Open: from 9:00 to 12:00 and from 13:00 to 17:00

Excluding Saturday, Sunday, Holidays and between 31 December and 3 January.

12. Admitted Personal Information Protection Association and Contact for Resolution of Complaints

The Branch is a member of the Foreign Non-Life Insurance Association of Japan, Inc. (FNLIA), an admitted personal information protection association.

Home Page: <https://www.fnlia.gr.jp/>

<About our designated Alternative Dispute Resolution (ADR) Organization>

We have the Basic Contract on Procedure and Practice with the legally authorized ADR Organization.

In case a dispute with us cannot be resolved, you are entitled to make a statement to the ADR. For further details, please refer to the ADR Home Page below.

Hoken Ombudsman, Inc.

Tel: 03-5425-7963

Open: from 9:00 to 12:00 and from 13:00 to 17:00

Excluding Saturday, Sunday, Holidays, Year end and New Year days etc.

Home Page: <https://www.hoken-ombs.or.jp/>