Version 1.0

Effective:
May 2018

# Allianz Privacy Standard

## Purpose of this document

This document describes the Allianz Privacy Standard and provides you with information on the rules governing the international transfer of personal data between Allianz Group companies operating in the European Economic Area (EEA) and Allianz Group companies outside that area. This APS also describes your rights in respect of such transfers, what to do if you want to exercise your rights or complain about such transfers, and how to contact us.

Allianz

## Contents

# A. Introduction

- This is the public version of the Allianz Privacy Standard (APS). The APS contains the Binding Corporate Rules (BCRs) of Allianz, which were approved by national data protection authorities in the European Economic Area (EEA). These authorities include the lead data protection authority for the Allianz Group, the Bavarian Data Protection Authority (BayLDA).

- BCRs were developed by the EEA to allow multinational corporations to make intra-organizational transfers of personal data across borders in compliance with EEA data privacy & protection laws and regulations. In principle, EEA laws and regulations do not allow the transfer of personal data from the EEA to Asia, the U.S. and other regions. With BCRs, companies overcome that restriction.

- Attaining BCR approval emphasizes the commitment of Allianz to maintaining the trust of our customers, employees and business partners regarding how we use their personal data.

- The APS addresses the processing activities that Allianz conducts as a data controller while performing our business activities. The APS covers the personal data of current, former and prospective employees. It also covers the data of agents, brokers, intermediaries, pension trustees, suppliers and service providers, shareholders and other business partners. It also covers customers, corporate clients, customer and corporate client representatives, and other third parties.

- Allianz Group companies are required to implement the APS. This standard and an up-to-date list of Allianz Group companies who have committed to comply with the APS is available on https://www.allianz.com/en/info/privacy-statement/.

## Key Terms

| Term | Description |
|---|---|
| **Allianz Group** | The Allianz Group encompasses Allianz SE and any affiliated company according to Section 15 of the German Stock Corporation Act (AktG). |
| **APS** | APS refers to the Allianz Privacy Standard, which contains the Binding Corporate Rules of Allianz, as well as the minimum requirements for data privacy & protection compliance across the Allianz Group. |
| **Binding Corporate Rules (BCRs)** | Are the legally recognized mechanism for legitimizing and facilitating transfers of personal data originating from or processed in the EEA within a corporate group. |
| **Data Controller** | A data controller is a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes ("why") and the means ("how") of the processing of your personal data. If two or more data controllers jointly determine the purposes and means of the processing, they are considered joint controllers and must cooperate in a transparent manner to ensure adherence to the APS. |
| **Data Processor** | Is a natural or legal person which processes your personal data on behalf of a data controller. |
| **EEA** | The European Economic Area consist of the countries forming part of the European Union, as well as Iceland, Liechtenstein and Norway. |
| **Employees** | Covers all employees, managers, directors and executive board members of an Allianz Group company. |
| **Group Chief Privacy Officer** | Is the head of Group Privacy & Data Protection of the Allianz Group. The person is appointed by the Allianz SE Board of Management. |
| **Group Privacy & Data Protection** | Refers to the Group Privacy & Data Protection department at Allianz SE. |
| **Individual** | An individual is defined as an identified or identifiable natural person to whom personal data relates. An identifiable natural person is one who can be identified, directly or indirectly, particularly by reference to an identifier such as a name, identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. In the APS, this refers to employees and related staff, customers, business partners or any other third parties whose personal data are processed. |
| **International Transfers** | Mean a disclosure of personal data, via physical transmission or remote access, to non-EEA Allianz Group companies that are legally bound by the APS. |
| **Personal Data** | Refers to any information relating to an individual. |

| Term | Description |
|---|---|
| **Personal Data Loss** | Personal data loss means all cases of data loss, leakage or breach, which include or might include personal data. |
| **Processing** | Means any operation or set of operations performed on your personal data or on sets of your personal data. This can be by automated or by other means. It covers such activities as the collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making data available. It also refers to the alignment or combination, restriction, erasure or destruction of data. |
| **Profiling** | Profiling is any form of automated processing of your personal data consisting of the use of your personal data to evaluate certain personal aspects relating to you. This may refer to use for analysis or to predict aspects concerning your performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements. |
| **Recipient** | A recipient is a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. |
| **Sensitive Personal Data** | Means personal data that can reveal your racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership. It also refers to the processing of your genetic data and biometric data to uniquely identifying you, as well as data concerning your health or data concerning your sex life or sexual orientation. |

# B. Principles for Data Privacy & Protection Compliance

Allianz Group companies observe the following principles when processing personal data that are subject to EEA data privacy & protection laws and regulations.

## I. Due Care

We process your personal data with due care, in a fair, lawful and transparent way.

## II. Data Quality

### 1. Purpose Limitation

We only process your personal data to fulfill our specific, clear and legitimate business purposes. We may make specific, clear and legitimate changes to our business purposes.

Any new business purposes will be compatible with the initial purposes for which we collected your personal data, unless you agree to your data being processed for other purposes. We will inform you about any such changes.

### 2. Data Minimization & Accuracy

If you inform us of changes in your personal data or we make changes as a part of our processing of your personal data, we ensure that:

- Your personal data are up-to-date and that if any personal data are inaccurate, that these are promptly erased or rectified as is appropriate bearing in mind why we are processing your personal data.
- Any updates to your personal data are reflected across our systems and databases whether internal or external.
- Your personal data are adequate and limited to what is necessary for our business purposes.

### 3. Storage Limitation

We only keep your personal data for as long as we need to meet our business purposes or as required by law.

We appropriately dispose of and/or archive your personal data when we no longer need it. Alternatively, we anonymize your personal data in such a way that you can no longer be identified if we wish to retain it beyond that point in time.

## III. Transparency & Openness

Generally, we collect your personal data directly from you. If we collect personal data from other sources, it is because this is reasonable and permitted by law. The information we provide to you differs depending on the source of the personal data. The following table sets out the information we provide you with when we collect your personal data either directly from you or from another source:

| | Data collected directly from you | Data collected from third parties |
|---|---|---|
| Which Allianz Group company (or representative) is responsible for handling your personal data (data controller). | ✓ | ✓ |
| Who you can contact with queries or concerns about the handling of your personal data. This will usually be the data protection officer or data privacy professional. | ✓ | ✓ |
| Why we need to process your personal data and the legal basis that allows us to do so. | ✓ | ✓ |
| If we believe processing your personal data is in our legitimate interest or that of a third party and details about such interest. | ✓ | ✓ |
| The type of personal data we process (for example, your name or date of birth). | | ✓ |
| The companies and people, or categories of companies and people we share your personal data with. | ✓ | ✓ |
| The steps we take to protect your personal data when we send them to other companies or people located outside the EEA, as well as how to obtain further information about such steps. | ✓ | ✓ |
| How long we keep your personal data for or if it's not possible, how we decided on this period. | ✓ | ✓ |
| The rights you have in relation to your personal data. | ✓ | ✓ |
| Your right to decide – at any time – that you no longer consent to us processing your personal data if you had previously given us your consent. However, any processing that we performed before will not be affected by your decision to revoke your consent. | ✓ | ✓ |
| Your right to complain to a relevant data protection authority in the EEA. | ✓ | ✓ |
| How we obtained your personal data and whether they were obtained from publicly accessible sources. | | ✓ |

| | Data collected directly from you | Data collected from third parties |
|---|---|---|
| If we collect your personal data because it is required by laws or regulations, by a contract signed between us or if we need them before we enter into a contract with you. We will also tell you if you are obliged to provide your personal data and of the possible consequences of not doing so. | ✓ | |
| If we use your personal data to make decisions about you automatically without human involvement, including if we use your personal data to make evaluations of personal aspects relating to you. We will also give you further information about the significance of these decisions, how they are made and their potential consequences. | ✓ | ✓ |

We provide you with this information when we collect your personal data. If this is not possible, then we will inform you:

- Within one month of collecting your personal data
- When we first communicate with you (if we use the personal data to communicate with you), or
- If disclosure to another recipient is planned, by the time your personal data are first disclosed

In certain circumstances we do not need to inform you. For example, if you know this information already or we are legally required to collect or share your personal data.

## IV. Lawfulness of Processing

### 1. Lawful Basis for Processing Your Personal Data

We only use your personal data if we have a lawful basis to do so. Where processing is necessary, these reasons include the need to:

- Create a contract with you or to take steps at your request before entering into a contract
- Comply with our legal obligations
- Protect your vital interests or those of another individual
- Perform a task in the public interest or to exercise an official authority vested in us, or
- Undertake actions for our legitimate business interests or the business interests of a third party, except if these legitimate interests are overridden by your interests or fundamental rights and freedoms

We may also process your personal data with your consent.

### 2. Consent

If we process your personal data based on your consent, we:

- Ensure that the wording and format used to collect your consent is clear and easy to understand, and that your consent is freely given, specific, informed and clear
- Have processes to record the giving and withdrawal of your consent and ensure that you can withdraw your consent easily. We will also inform you of this withdrawal right before you give consent
- Ensure that if your consent is collected as part of a written declaration that also concerns other matters, such as a contract, the request for consent in the written declaration is presented in a manner clearly distinguishable from the other matters.

### 3. Sensitive Personal Data

We only process your sensitive personal data if the processing is necessary for one of the following reasons. For:

- You or us to perform or exercise rights under employment and social security and social protection laws and regulations
- Preventive or occupational medicine health purposes, such as the assessment of the working capacity of an employee, medical diagnosis, health or social care, and activities of health professionals
- The public interest in terms of public health, if required by EEA law and regulations
- Reasons of substantial public interest, if required by EEA laws and regulations
- Archiving purposes in the public interest, scientific or historical research purposes or statistical purposes if required by EEA laws and regulations
- Processing relating to your sensitive personal data which you have made public
- Purposes to protect your vital interests or those of another individual if you are physically or legally not able to give consent, or
- Legal claims.

Alternatively, we process your sensitive personal data if you explicitly consent to its processing for one or more purposes, unless this is prohibited by EEA laws and regulations.

### 4. Personal Data Related to Criminal Convictions & Offences

We only process personal data relating to criminal convictions and offences, or related security measures, if it is permitted or required by EEA laws and regulations providing for adequate safeguards for your rights and freedoms.

## V. Relationship with Data Processors (for example, service providers working for us)

We only allow data processors acting on behalf of Allianz Group companies to collect and process your personal data if they enter into a written agreement with us outlining data privacy & protection requirements.

To ensure the quality of this process, we:

- Conduct due diligence checks and risk assessments to evaluate data processors to ensure they meet our security and confidentiality obligations and protect your personal data

- Periodically monitor data processors to verify on-going compliance with their data privacy & protection obligations.

## VI. Transfers & Onward Transfers

We may transfer your personal data from within the EEA to Allianz Group companies outside the EEA if they comply with the rules set out in the APS.

Transfers of your personal data to Allianz Group companies outside the EEA that are not covered by the rules of the APS, as well as transfers to data controllers or data processors that are not members of Allianz Group, are only permitted if at least one of the following conditions are met:

- The company is in a country where the European Commission has acknowledged the adequacy of that country's privacy & data protection laws and regulations.
- The company your personal data are transferred to provides appropriate safeguards in respect of that personal data. For example, if that company has signed data privacy & protection clauses that have been adopted by the European Commission or a data protection authority.
- In the specific and limited circumstances allowed by applicable EEA data privacy & protection laws and regulations. For example, with your explicit consent or if the transfer is necessary for the performance of a contract between us, or
- As a final resort, if the transfer is necessary for our compelling legitimate business interests provided that certain requirements are met (for example, the transfer is limited and not repetitive and there are no overriding reasons preventing the transfer). In these cases, we normally inform a data protection authority about the transfer before it happens.

## VII. Security & Confidentiality

We handle your personal data in accordance with the information security policies and standards of Allianz and in accordance with the laws and regulations that apply to us.

We adopt appropriate technical and organizational security safeguards to protect your personal data against risks that may result from improper use, particularly, against the accidental or unlawful destruction, alteration or loss, as well as unauthorized disclosure of or access to your personal data. The measures depend on factors such as the state of the art, nature and scope of the processing and level of risk, but may include:

- Using encryption, anonymization and partial anonymization of your personal data, if appropriate
- Regularly testing, assessing and evaluation of the effectiveness of security measures for ensuring the security of the processing
- Maintaining business continuity and disaster recovery plans and contingencies including ongoing confidentiality, integrity, availability and resilience over systems and services.

## VIII. Personal Data Loss

We will inform you – without undue delay – if a personal data loss incident is likely to result in a high level of risk to your rights and freedoms, including the following specifics:

- Nature of the personal data loss incident

- Likely consequences of the personal data loss incident
- Measures we are taking or plan to take to address the personal data loss incident, including, if appropriate, measures to mitigate its impact.

We will not inform you if:

- Our security measures render the personal data inaccessible or unusable to any person who is not authorized to access it (for example, the personal data are encrypted)
- We take subsequent measures to ensure that any high-level risks to your rights and freedoms are unlikely to happen, or
- It involves a disproportionate effort to contact every affected person individually. In such cases we will issue a public communication or similar measure to ensure that you are informed in an equally clear and effective way.

## IX. Privacy by Design & Default

### 1. Privacy by Design

We consider the principle of privacy by design when designing or changing an aspect that impacts upon the processing of personal data (for example, developing a new product, service or information technology system) to help us:

- Identify and limit the data protection impacts and risks of processing
- Comply with the requirements of the APS and with legal obligations affecting the processing
- Limit the data we collect or identify different ways that lessen the impact upon data privacy & protection while meeting the same business goal.

### 2. Privacy by Default

We use appropriate technical and organizational measures to ensure that, by default, we only collect and process personal data needed for our business purposes. We also use this principle to embed data privacy & protection controls into our processing activities, which means that your personal data will not be published or shared by default.

## X. Cooperation with Data Protection Authorities

We cooperate with EEA data protection authorities by:

- Making the necessary personnel available for liaison with EEA data protection authorities
- Complying with their advice on any matter regarding the rules for international transfers.

# C. Your Rights

You rights are summarized below. If you exercise your rights, make any request or have a complaint, these are handled in accordance with Section C.VI (Handling your Requests & Complaints).

## I. Requests to Access, Rectify or Erase

### 1. Access Request

You have the right to ask us whether we hold any personal data relating to you and, if we do, to be provided with a copy of that personal data in electronic form, unless you want to receive it in another way (for example, a paper copy). In addition, you can ask us for information on how we use your personal data, who we share it with, how long we keep it, where it is stored, and other information to help you understand how we use it.

### 2. Rectification Request

You have the right to ask us to correct your personal data (including by means of providing a supplementary statement) if it is inaccurate and to have incomplete personal data updated without undue delay. If we cannot correct the personal data, we include a note on our files regarding your request to correct your personal data.

### 3. Erasure Request

You have the right to ask us to erase your personal data if:

- Your personal data are no longer necessary for the purpose(s) they were collected for
- Your personal data have been unlawfully processed
- Your personal data must be erased to comply with an EEA law or regulation
- The personal data relates to a child or an individual whose personal data were collected when he/she was a child in relation to services provided via the internet, websites or apps
- You withdraw your consent for the processing of the personal data (and if this is the only basis on which we are processing your personal data)
- You object to processing that is based on our legitimate interests, provided there are no overriding legitimate grounds for continued processing, or
- You object to processing for direct marketing purposes.

If we have made the personal data concerned public, we also take reasonable steps to inform other data controllers processing the data so they can seek to erase links to or copies of your personal data.

We may refuse to act on your request to erase your personal data if the processing of your personal data is necessary:

- To exercise our right of freedom of expression and information
- To comply with EEA laws and regulations
- For the performance of a task carried out in the public interest or to exercise official authority vested in us
- To establish, exercise or defend legal claims.

In these cases, we can restrict the processing instead of erasing your personal data if requested to do so by you. See Section C.III for more details.

## II. Requests to Object

You have the right to object at any time to the processing of your personal data if we process it based on our legitimate interests. This includes any so-called “profiling”. Our privacy notice

informs you when we rely on legitimate interests to process your personal data. In these cases, we will stop processing your personal data unless we can demonstrate compelling legitimate reasons for continuing the processing. We may reject your request if the processing of your personal data is needed to establish, exercise or defend legal claims.

You have the right to object at any time if we process your personal data for direct marketing purposes. You may also object at any time to profiling supporting our direct marketing. In such cases, we will stop processing your personal data when we receive your objection.

## III. Requests to Restrict

You have the right to ask us to restrict the processing of your personal data if:

- You contest the accuracy of your personal data and we are in the process of verifying the personal data we hold
- The processing is unlawful and you do not want us to erase your personal data
- We no longer need your personal data for the original purpose(s) of processing, but you need them to establish, exercise or defend legal claims and you do not want us to delete the personal data as a result, or
- You have objected to processing carried out because of our legitimate interests (see previous section), while we verify if our legitimate grounds override yours.

If processing is restricted, we may process your personal data (excepting for storage purposes), only:

- If you have given us your consent
- For establishing, exercising or defending legal claims
- For protecting the rights of another natural or legal person, or
- For reasons of important public interest as defined under applicable EEA laws and regulations.

Once processing is restricted following your request, we will inform you before we lift the restriction.

## IV. Requests for Portability

If our processing is performed by computer and is necessary to fulfil a contract with you, or is based on your consent, you have the right to:

- Receive any personal data you have provided to us in a structured, commonly used and machine-readable electronic format
- Send your personal data to another organization or have us do so for you if it is technically feasible for us to do so.

If your request relates to a set of personal data that also concerns other individuals, the fact that you request that we port this data as described above does not preclude those individuals from exercising their own rights regarding their personal data.

Even if you request the portability of your personal data, you retain your right to also request their erasure in accordance with Section C.I.3 above.

## V. Requests to Object to Automated Decisions

Generally, you have the right to object to any decision producing a legal effect concerning you (such as, cancellation of your contract) or which otherwise significantly affects you (for example, refusal of your online insurance application) if this is based solely on the automated processing of your personal data. This includes automated decisions based on profiling.

We may refuse your request if the decision in question is:

- Necessary to enter into a contract with you, or for the performance of your contract with us
- Permitted by EEA laws and regulations, or
- Based on your explicit consent.

We will only make decisions relying solely on automated processing that involve your sensitive personal data if you have given your explicit consent or the processing is necessary for reasons of substantial public interest, based on applicable EEA laws and regulations, and we safeguard your rights, freedoms, and legitimate interests.

## VI. Handling Your Requests Relating to Your Personal Data

### 1. Confirmation of Your Identity

We want to ensure that we do not give your information to someone not entitled to it. Therefore, we may request additional information from you to confirm your identity before we handle your request.

### 2. Timelines to Handle Requests

When we receive a request from you:

- We inform you of any action taken without undue delay. At the latest, this will be within one month of receiving the request.
- We may extend the time to respond by a further two months depending on the nature of your request. We will notify you of any extension within one month together with the reasons for the extension.
- We will inform you as soon as we can (at the latest within one month) if we decide not to comply with your request together with our reasons for the refusal. You will also receive information about your right to complain to an EEA data protection authority, and/or your right to seek judicial remedies.

### 3. Form of Response

If you make an electronic request, we aim to respond electronically, unless you request us to respond in a different way.

### 4. Costs

We generally do not charge for your request. However, we may need to do so if:

- Your request is unfounded or excessive, for example, if the request is repetitive, or
- You ask for additional copies of personal data that we have already provided to you.

### 5. Refusal to Fulfil Your Request

We may refuse to fulfil your request if:

- The request is unfounded or excessive, for example, if the request is repetitive
- Our processing does not require us to identify you and we can demonstrate that we cannot identify you, or
- EEA laws and regulations prevent us from fulfilling your request, for example, if a court or regulatory authority has imposed a legal hold on us.

### 6. Notification of Change to Recipients of Your Personal Data

We inform any third parties with whom we share your personal data, such as vendors or service providers, of changes due to the erasure, rectification or restriction of processing of your personal data, unless this is impossible or involves disproportionate effort. We will inform you who those recipients are if you request this.

## D. International Transfers of Your Personal Data

### I. Your Complaints and How we Handle Them

We take any complaint about the way in which your personal data have been handled under the rules for international transfers seriously. You can register a complaint by sending an email to privacy@allianz.com.

We will:

- Acknowledge your complaint within two weeks of receipt, endeavor to resolve it and respond to you as soon as possible, and in any event, within two months. We will inform you of the procedure and timelines for responding, and will keep you updated during this period
- Investigate the circumstances relating to your complaint and collect information so as to provide a response
- Promptly escalate your complaint to the Group Chief Privacy Officer if, during investigation, the Allianz personnel with responsibility for handling the complaint anticipate that the 2 month-deadline cannot be met. We will inform you of this and our estimate of how long it will take to handle your complaint (in any event, within two months of escalation)
- Resolve your complaint if it is upheld and inform you of the action we have taken. You can escalate your complaint to the Group Chief Privacy Officer if you are not satisfied with the outcome
- Inform you if your complaint is not upheld and of your right to escalate your complaint to the Group Chief Privacy Officer.

### II. Your Third-party Beneficiary Rights Relating to International Transfers of Your Personal Data

The rules on international transfers under EEA data privacy & protection laws and regulations require that when personal data are transferred from an Allianz Group company within the EEA to an Allianz Group company outside the EEA, individuals whose personal data are transferred must be able to benefit from certain rights in respect of that data as third-party beneficiaries. As a result, if your personal data are transferred from an Allianz Group company within the EEA to Allianz Group companies outside the EEA, you can enforce the following as third-party beneficiary rights:

- Due Care (Section B.I)
- Data Quality (Section B.II)
- Transparency & Openness (Section B.III)
- Lawfulness of Processing (Section B.IV)
- Relationship with Data Processors (Section B.V)
- Transfers & Onward Transfers (Section B.VI)
- Security & Confidentiality (Section B.VII)
- Personal Data Loss (Section B.VIII)
- Privacy by Design & Default (Section B.IX)
- Cooperation with Data Protection Authorities (Section B.X)
- Requests to Access, Rectify or Erase (Section C.I)
- Requests to Object (Section C.II)
- Requests to Restrict (Section C.III)
- Requests for Portability (Section C.IV)
- Requests to Object to Automated Decisions (Section C.V)
- Handling Your Requests Relating to Your Personal Data (Section C.VI)
- Your Complaints and How we will Handle them (Section D.I)
- Your Third-party Beneficiary Rights Relating to International Transfers of Your Personal Data (Section D.II)
- Application of Laws and Regulations (Section E)

Enforcing a third-party beneficiary right means you can take action against an Allianz Group company subject to the rules of the APS, in accordance with the liability rules set out below, even if you do not normally deal with them and you do not have a contract with that company. This includes recourse to judicial remedies for any violation of your rights, including redress and if appropriate, compensation.

In all cases, you have the right to bring a claim for a violation of your third-party beneficiary rights in accordance with this section. You can bring a claim before the following:

- The courts in the jurisdiction of the Allianz Group company located in the EEA that transferred your personal data outside of the EEA
- The courts in the jurisdiction where you have your habitual residence in the EEA, and/or
- The EEA data protection authority for the EEA country where you have your habitual residence or your work, or where the alleged violation took place.

If an Allianz Group company in the EEA (the “exporter”) shares your personal data with another Allianz Group company outside the EEA (the “importer”), that results in a violation of the APS affecting your personal data, you can bring a claim against the exporter. The liability of the exporter is limited to direct material and non-material damages resulting from the violation.

The burden of proof rests with Allianz to prove it is not responsible for the violation or that no violation took place.

## E. Application of Laws and Regulations

If any part of the APS is less strict than local laws or regulations, such local laws or regulations will apply on top of these requirements.

We will seek to resolve any conflict between the provisions of the APS and local laws and regulations to determine appropriate actions. We will consult with EEA data protection authorities in the case of legal uncertainty.

## F. Updates to this Document

We will adjust this document to reflect any changes made to the APS. We will specify the date on which this document was last reviewed and the dates and reasons for any changes.

| Version | Revision Date | Reason for Changes |
|---|---|---|
| [●] | [●] | [●] |

If you have any questions regarding the APS, please contact our Group Chief Privacy Officer on privacy@allianz.com.