Version 5.0

Effective: 01.01.2023

Allianz Privacy Standard (APS)

Classification: Internal

Authorization:

The content of this document has been reviewed and approved as follows:

Version	Valid from	Authorized by			Taken notice by
		Group Policy Team	Allianz SE Board Member	Management Board Committee	Allianz SE Board of Management
5.0	01.01.2023	-	Renate Wagner		08.12.2022

Executive Summary

I. Allianz is strongly committed to conducting business in full compliance, and in accordance with applicable data privacy and protection laws and regulations. In doing so Allianz strives to safeguard the Personal Data of Individuals, protect the Allianz Group, and promote confidence in Allianz as a trusted provider of financial products and services.

II. The Allianz Data Privacy and Protection Framework ("Framework") comprises:

- The *Allianz Privacy Standard* contains the global minimum requirements applicable within the Allianz Group for the Processing of Personal Data, as well as additional requirements for EEA Processing; and
- Functional Rules that further specify data privacy and protection requirements. These relate to *Privacy Impact & Ethics Assessments and Records of Processing*, the handling of *Subject Access Requests and Complaints*, and *Personal Data Incident Management*.

III. The *Allianz Privacy Standard* applies to the Allianz Group. Separate and in addition to the *Allianz Privacy Standard*, the Allianz Group Binding Corporate Rules are Allianz's legally recognized binding mechanism to legitimize and facilitate cross-border transfers of Personal Data originating from or processed in the EEA within the Allianz Group ("Binding Corporate Rules"). The Binding Corporate Rules apply to Allianz legal entities which are signatories to the Intercompany Agreement.

IV. The *Allianz Privacy Standard* does not cover information security, records retention and deletion, non-data privacy and protection related incident management and the general protection of business secrets which are subject to the requirements of other Allianz corporate rules.

V. The Allianz SE Board of Management noted the *Allianz Privacy Standard* on May 28, 2018. The APS applies to all OEs(including the legal entities part of the OE) and Employees, who are legally bound to comply with its requirements. Non-compliance with the APS may expose Employees to legal consequences, including disciplinary action, and in very severe cases, up to and including termination.

VI. OEs may develop equivalent rules and procedures to align with the requirements of the *Allianz Privacy Standard* to their respective business structure or model. Any material deviations from the *Allianz Privacy Standard* must be pre-aligned with Group Privacy, and properly documented.

VII. The *Allianz Privacy Standard* is the divisional responsibility of the member of the Allianz SE Board of Management with responsibility for the data privacy and protection function.

Contents

A. Introduction

I. Rationale

1. Allianz commits to protecting the privacy and data protection rights of its Employees, customers, business partners and third-parties ("Individuals"). This *Allianz Privacy Standard* ("APS") is designed to facilitate adherence to applicable data privacy and protection laws and regulations which govern the Processing and transfer of Personal Data. In particular, the APS provides a framework for the Processing of Personal Data subject to EEA laws and regulations within the Allianz Group.

2. The APS sets out global minimum data privacy and protection requirements for the Processing of Personal Data by all OEs ("Global Minimum Requirements", icon 1 below). In addition, the APS sets out minimum requirements for the Processing of Personal Data subject to EEA laws and regulations ("Requirements for EEA Processing", icon 2 below). Where applicable, the Requirements for EEA Processing apply in addition to the Global Minimum Requirements. These icons appear as follows in the APS:

   1 Apply to Processing of Personal Data generally ("Global Minimum Requirements")

   2 Apply to Processing of Personal Data subject to EEA laws and regulations ("Requirements for EEA Processing")

   An overview of all requirements is provided in Annex E (APS Requirements Overview).

3. In addition to the APS, the *Allianz Group Binding Corporate Rules* ("BCRs") are the legally recognized mechanism to legitimize and facilitate, across Allianz Group, transfers of Personal Data originating from, or processed in, the EEA. The requirements for BCR transfers are separately set forth, but obligate Allianz Group legal entities which are signatories to the Intercompany Agreement ("BCRs Parties") and receive EEA Personal Data, to adhere to the Requirements for EEA Processing, as well as certain additional obligations, with respect to the Processing of that EEA Personal Data. BCR Parties shall ensure all Employees of BCRs Parties adhere to and are legally bound comply with the BCRs.

4. As concerns Allianz's legally recognized mechanism to legitimize and facilitate cross-border transfers of Personal Data originating from or processed in the EEA within the Allianz Group, the BCRs shall prevail in the event of ambiguity between the BCRs and the APS.

5. The APS supersedes and replaces the *Allianz Privacy Standard* 4.0 dated January 1, 2022. The APS is supplemented by Functional Rules referred to in Chapter F. The APS and its corresponding Functional Rules together form the Allianz Data Privacy and Protection Framework (the "Framework").

6. The APS applies to Allianz Group, and covers all OEs (including the legal entities part of the OE. OEs shall ensure Employees are legally bound to comply with its requirements. Non-compliance with the APS and the BCRs, where applicable, may expose Employees to consequences, including disciplinary action, and in very severe cases up, to and including termination.

7. OEs must implement the Framework effectively, consistent with legal requirements in their respective jurisdictions and communicate the Framework to all relevant addressees.

8. By default, the APS requirements apply to both OEs acting as Data Controllers and OEs acting as Data Processors on-behalf of OE Data Controllers, unless stated otherwise. Besides where Requirements for EEA Processing apply only to OE Data Controllers, OE Data Processors must adhere to the standards imposed on those OE Data Controllers, and facilitate the OE Data Controllers' ability to comply with such standards.

9. The APS does not cover information security, records retention and deletion, non-data privacy and protection related incident management and the general protection of business secrets which are subject to the requirements of other Allianz Corporate Rules.

10. If any part of the APS is less strict than local laws or regulations, such local laws or regulations will prevail. In the event of any ambiguity between the Global Minimum Requirements and the Requirements for EEA Processing, the Requirements for EEA Processing Transfers will prevail. In the event of any uncertainty, the respective OE's Data Privacy Professional ("DPP") / Data Protection Officer ("DPO") (whose roles and responsibilities are defined in Chapter E, Section II.2 below) must consult with Group Privacy ("GP") to resolve the conflict.

11. The Group Chief Privacy Officer ("GCPO") may at their discretion waive in whole or in part any Global Minimum Requirement for any non-EEA OE Data Controller or Data Processor for which the Requirements for EEA Processing are inapplicable. The GCPO must document in writing any exception to the Global Minimum Requirements and the reasoning supporting this decision.

II. Authorization and Updates

The member of the Allianz SE Board of Management in charge of business division H6 is assigned overall responsibility for GP until January 1, 2023, at which time, overall responsibility for GP will move to the member of the Allianz SE Board of Management in change of business division H4. GP is the owner of the APS and is assigned responsibility to maintain and update the APS. The APS must be reviewed at least once per year. The APS must be approved by the member of the Allianz SE Board of Management in charge of GP and duly noted by the Allianz SE Board of Management.

The Framework is available in the Corporate Rule Book on Allianz Connect.

The APS (version 5.0) will apply as of January 1, 2023, following notification to the Allianz SE Board of Management. The APS (version 5.0) supersedes and replaces the *Allianz Privacy Standard* 4.0, dated January 1, 2022.

B. Principles for Data Privacy and Protection Compliance

I. Due Care

1 2 OE Data Controllers must Process Personal Data with due care and lawfully, fairly, and in a transparent manner.

II. Data Quality

1. Purpose Limitation

1 2 #### 1.1. Global Minimum Requirements

OE Data Controllers must Process Personal Data for specified, explicit and legitimate business purposes and in accordance with the following:

- Applicable laws and regulations, including professional confidentiality;
- Information security requirements contained in the Allianz Group Information Security Framework (GISF); and
- Data retention and deletion requirements contained in the *Allianz Standard for Information and Document Management* (ASIDM).

OE Data Controllers must Process Personal Data only to the extent that is essential to fulfill the specified business purposes.

OE Data Controllers may make subsequent changes to the specified business purposes provided such changes are specified, explicit, and legitimate.

2 #### 1.2. Additional Requirements for EEA Processing

OE Data Controllers may make subsequent changes to the specified business purposes provided this is not incompatible with the initial purposes.

1 2 ### 2. Data Minimisation and Accuracy

OE Data Controllers must ensure that:

- Personal Data are kept up-to-date and that any inaccuracies are promptly erased and rectified having regard to the purposes for which they are Processed;
- Any updates to Personal Data are reflected in all systems and databases whether internal or external; and
- Personal Data are adequate and limited to what is necessary for the purposes for which the Personal Data are to be Processed.

1 2 ### 3. Storage Limitation

OE Data Controllers must store Personal Data so long as is necessary to fulfill specified business purposes or as required by applicable laws and regulations, and in

accordance with Allianz data retention and deletion requirements contained in the ASIDM.

OE Data Controllers must appropriately dispose of and archive Personal Data in accordance with applicable laws and regulations, and Allianz data retention and deletion requirements contained in the ASIDM.

As an alternative to disposal, OE Data Controllers may anonymize Personal Data.

III. Transparency and Openness

1. Global Minimum Requirements

OE Data Controllers must inform Individuals, in accordance with applicable laws and regulations, at the time of collection and in clear and accessible terms, of the purposes for which their Personal Data are collected, how they are to be Processed and, if applicable, to whom they will be transferred.

OE Data Controllers must ensure that Personal Data are primarily collected directly from the Individual concerned and only collected from third-parties or other sources, provided this is reasonable and permitted by applicable laws and regulations.

2. Additional Requirements for EEA Processing

2.1. Information collected from the Individual

OE Data Controllers must provide Individuals with the information set out below in writing or by other means including, where appropriate, in electronic form. It must be provided in a concise, transparent, intelligible and easily accessible form, and using clear and plain language:

- The name and contact details of the OE Data Controller or its Representative;
- The contact details of the OE DPP/DPO, where applicable;
- The purposes of the Processing for which the Personal Data are intended and the legal basis for the Processing;
- The legitimate interest pursued by the Data Controller or by a third-party, where such interest provides the legal basis for the Processing;
- The recipients or categories of recipients of the Personal Data;
- In case of transfers to non-EEA countries, the fact that the OE Data Controller intends to transfer Personal Data to a third country and the existence or absence of an adequacy decision by the European Commission, or the suitable safeguards implemented to protect the Personal Data transferred, and the means by which an Individual can obtain a copy of them or where they have been made available;
- The period for which the Personal Data will be stored or, if not possible, the criteria used to determine this period;
- The existence of Individuals' rights to:
  - Access, rectify and erase Personal Data;
  - Restrict Processing;

- Data portability;
- Object to Processing. This right must be explicitly brought to the Individual's attention, clearly and separately from any other information, where the Processing is based on the Data Controller's legitimate interest or where Personal Data are Processed for direct marketing purposes;
- Withdraw consent at any time where consent provides the legal basis for the Processing of Personal Data or Sensitive Personal Data. Such withdrawal must not affect the lawfulness of the Processing carried out before the Individual's request for withdrawal of their consent; and
- Lodge a complaint before a Competent Supervisory Authority, in particular in the Member State of their habitual residence, place of work, or place of the alleged infringement;

- Whether the provision of Personal Data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the Individual is obliged to provide the Personal Data, and of the possible consequences of failure to do so; and
- The existence of automated decision-making, including Profiling, and meaningful information about the logic involved, as well as the significance and envisaged consequences of such Processing for the Individual.

OE Data Controllers intending to Process Personal Data for a purpose other than the initial purpose must inform the affected Individuals prior to the further Processing with information on that other purpose, as well as any relevant information listed above.

2.2. Information not collected from the Individual

Where Personal Data are not obtained from Individuals, OE Data Controllers must provide them with details of the following, in addition to the information listed in Chapter B, Section III.2.2.1. above:

- The categories of Personal Data concerned; and
- The source of the Personal Data and, if applicable, whether from publicly accessible sources.

OE Data Controllers must provide such information to Individuals:

- Within one month of obtaining the Personal Data, having regard to the specific circumstances in which the Personal Data are processed;
- If the Personal Data are to be used to communicate with Individuals to whom the Personal Data relate, at the latest at the time of first communication with those Individuals; or
- If a disclosure to another recipient is envisaged, at the latest when the Personal Data are first disclosed.

OE Data Controllers intending to Process Personal Data for a purpose other than the initial purpose must inform the affected Individuals prior to the further Processing with information on that other purpose, as well as any relevant information listed above.

OE Data Controllers do not need to provide such information to Individuals if:

- They already have such information;
- It would prove impossible or involve a disproportionate effort;
- Obtaining or disclosure of Personal Data is expressly required by applicable EEA laws and regulations; or
- The Personal Data must remain confidential subject to an obligation of professional secrecy required by applicable EEA laws and regulations.

IV. Lawfulness of Processing

1. Global Minimum Requirements

OE Data Controllers must only process Personal Data if there is a lawful basis for this as follows:

- The Processing is necessary to perform a contract to which the Individual is party, or in order to take steps at the request of the Individual prior to entering into a contract;
- The Processing is necessary to comply with a legal obligation laid down by applicable law to which the Data Controller is subject;
- The Processing is necessary to protect the vital interests of the Individual or of another natural person;
- The Processing is necessary to perform a task in the public interest or to exercise an official authority vested in the Data Controller laid down by applicable law to which the Data Controller is subject;
- The Processing is necessary for the legitimate interests of the Data Controller or a third-party, except where such legitimate interests are overridden by the Individual's interests or fundamental rights and freedoms which require protection; or
- With the consent of the Individual, where applicable subject to the conditions set out in Chapter B, Section IV.2 below.

2. Conditions for consent for EEA Processing

Where Personal Data are Processed on the basis of an Individual's consent, OE Data Controllers must:

- Ensure that consent is freely given, specific, informed, and an unambiguous indication of the Individual's wishes (by a statement or clear affirmative action) to agree to the Processing;
- Ensure that the Individual is able to withdraw their consent easily, and receives information of such ability prior to giving consent;
- Implement and maintain processes to record the giving and withdrawal of consent; and
- Ensure that if consent is given as part of a written declaration also concerning other matters, it is presented in a manner which is clearly distinguishable from other matters, in an intelligible form, using clear, and plain language.

3. Lawfulness of Sensitive Personal Data Processing for EEA Processing

OE Data Controllers must implement and maintain processes to identify where Sensitive Personal Data are Processed and ensure that Sensitive Personal Data are only Processed if:

- Processing is necessary:
  - For the Data Controller or Individual to perform or exercise specific rights under applicable employment and social security and social protection law in so far as it is permitted by applicable EEA laws and regulations;
  - To protect the vital interests of the Individual or of another natural person where the Individual is physically or legally incapable of giving consent;
  - To establish, exercise or defend legal claims, or whenever courts act in their judicial capacity;
  - For the purposes of preventive or occupational medicine, for the assessment of the working capacity of an Employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services under applicable EEA laws and regulations or pursuant to a contract with a health professional subject to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy;
  - For the public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of applicable EEA laws and regulations which provide for suitable and specific measures to safeguard the rights and freedoms of the Individual, in particular professional secrecy;
  - For reasons of substantial public interest, under applicable EEA laws and regulations, which must be proportionate to the aim pursued, respect the essence of the right to data privacy and protection, and provide for suitable and specific measures to safeguard the Individual's fundamental rights and interests; or
  - For archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with applicable EEA laws and regulations, which must be proportionate to the aim pursued, respect the essence of the right to data privacy and protection, and provide for suitable and specific measures to safeguard the Individual's fundamental rights and interests;
- Processing relates to Sensitive Personal Data which are manifestly made public by the Individual; or
- The Individual has given their consent to the Processing for one or more specific purposes, except where this is prohibited by applicable EEA laws and regulations.

4. Lawfulness of Processing for criminal convictions and offences for EEA Processing

OE Data Controllers may not process Personal Data relating to criminal convictions and offences or related security measures other than under the control of an official authority, or where the Processing is authorized by applicable EEA laws and

regulations providing for adequate safeguards for the rights and freedoms of Individuals.

V. Relationship with Data Processors

1. Global Minimum Requirements

Personal Data may only be Processed by Data Processors on behalf of OE Data Controllers by means of a written agreement.

OE Data Controllers must:

- Conduct due diligence checks and risk assessments to evaluate Data Processors in order to verify that such Data Processors can provide appropriate technical and organizational measures in accordance with the GISF to ensure a level of security appropriate to the protection level and confidentiality of the Processed Personal Data; and
- Periodically monitor Data Processors to verify on-going compliance with their contractual and compliance obligations.

2. Additional Requirements for EEA Processing

OE Data Controllers must:

- Ensure that such Data Processors can provide sufficient guarantees in respect of the technical and organizational measures governing the envisaged Processing, such that the Processing will meet the security and confidentiality requirements set out in Chapter B, Section VII.2.; and
- Where the prospective Data Processor is not a member of Allianz Group, enter into a written agreement with the prospective Data Processor, containing the applicable minimum requirements set out in Annex B (Minimum Requirements for Data Controller - Data Processor Contractual Relationships for EEA Processing); or, where the prospective Data Processor is an OE Data Processor, adhere to the Intra-Company Data Processing Terms as attached in Schedule 1 to Annex C of the BCRs or a data progressing agreement with materially similar terms..

VI. Transfers and Onward Transfers

1. Global Minimum Requirements

OE Data Controllers and OE Data Processors must only disclose, share, or transfer Personal Data to other OEs in accordance with the APS.

OE Data Controllers and OE Data Processors must only disclose, share, or transfer Personal Data to Data Controllers or Data Processors that are not members of Allianz Group in accordance with the APS, and on the basis of written contracts, unless such sharing or transfer is explicitly permitted by applicable laws and regulations. Where such disclosure, sharing, or transfer is done for purposes other than the specified business purpose, it must only be done if permitted by applicable laws or regulations, or with the Individual's explicit consent.

2. Additional Requirements for EEA Processing

OE Data Controllers and OE Data Processors may transfer Personal Data to non-EEA OEs (either acting as Data Controllers or Data Processors) that comply with the BCRs and that are party to an ICA.

Transfers of Personal Data to non-EEA OEs that are not party to an ICA, or from EEA OEs to non-EEA Data Controllers or Data Processors that are not members of Allianz Group, or onward transfers of Personal Data from non-EEA OEs to Data Controllers or Data Processors that are not members of Allianz Group, are permitted on the basis of the following:

- An adequacy decision issued by the European Commission;
- The Data Controller or Data Processor providing appropriate safeguards in respect of the Personal Data transferred (*e.g.*, via standard data protection clauses adopted by the European Commission or an EEA data protection authority) in accordance with applicable EEA laws and regulations;
- In the absence of an adequacy decision, or of appropriate safeguards:
    - The data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;
    - The transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;
    - The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;
    - The transfer is necessary for important reasons of public interest;
    - The transfer is necessary for the establishment, exercise or defence of legal claims;
    - The transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent;
    - The transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by Union or Member State law for consultation are fulfilled in the particular case; or
- As a final resort, if the transfer is necessary for the purposes of compelling legitimate interests pursued by the Data Controller provided:
    - The transfer is not repetitive and concerns only a limited number of Individuals;
    - The Data Controller’s legitimate interests are not overridden by the Individual’s interests or rights and freedoms;

- The Data Controller has assessed and documented all the circumstances surrounding the transfer and, on the basis of this, has provided suitable safeguards with regard to data privacy and protection; and
- The Data Controller informs the competent EEA data protection authority and the Individual of the transfer and the compelling legitimate interests.

VII. Security and Confidentiality

1. Global Minimum Requirements

OE Data Controllers and OE Data Processors must handle Personal Data in accordance with the Allianz Group Information Security Framework (GISF).

2. Additional Requirements for EEA Processing

OE Data Controllers and OE Data Processors must adopt security safeguards against risks presented by the Processing of Personal Data, particularly from loss, accidental or unlawful destruction, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored or otherwise processed.

Taking into account the state of the art, costs of implementation, nature, scope, context and purposes of Processing, and the severity and likelihood of risks to Individuals' rights and freedoms, OE Data Controllers and OE Data Processors must implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, such as:

- The anonymization of Personal Data;
- The pseudonymization and encryption of Personal Data;
- The ability to ensure the ongoing confidentiality, integrity, availability and resilience of Processing systems and services;
- The ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident;
- Processes for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures for ensuring the security of the Processing;
- Processes to ensure that any natural person acting under the authority of the Data Controller or the Data Processor who has access to Personal Data, does not Process Personal Data except on instructions from the Data Controller, unless they are required to do so by applicable EEA laws and regulations; or
- Business continuity and disaster recovery plans and contingencies.

VIII. Personal Data Incidents or Breaches

1. Global Minimum Requirements

OE Data Controllers and OE Data Processors must implement and maintain effective processes to ensure timely notification to the OE DPP/DPO in the event of a Personal Data Incident or Breach.

OE Data Controllers and OE Data Processors must inform GP of any communications to or from a responsible supervisory authority that triggers, or is likely to trigger, a regulatory inquiry into the data privacy and protection practices of the OE Data Controller or OE Data Processor and in no event may an OE Data Controller or OE Data Processor accept a regulatory penalty without prior consultation of GP.

Further requirements are set out in the *Functional Rule for Personal Data Incident Management*, *Allianz Standard for Protection and Resilience* (AZ P&R Standard), *Allianz Functional Rule for Protection & Resilience* (AZ P&R Functional Rule), and *Allianz Functional Rule for Information Security* (AFRIS), and in other Allianz policies and standards as may be communicated to OEs from time to time.

2. Additional Requirements for EEA Processing

OE Data Controllers and OE Data Processors must implement and maintain processes to assess applicable data privacy and protection notification obligations, including notification to competent EEA data protection authorities, Individuals, and Data Controllers.

2.1. Notification to the competent EEA data protection authority

OE Data Controllers must, without undue delay and, where feasible, no later than 72 hours on becoming aware of a Personal Data Breach that is likely to result in a risk to an Individual's rights and freedoms, document and notify the Personal Data Breach to the competent EEA data protection authority, and notify without undue delay the OE DPP/DPO and GP of the following:

- The nature of the Personal Data Breach, including where possible, the categories and approximate number of Individuals affected, the categories, and approximate number of Personal Data records concerned;
- The name and contact details of the OE DPP/DPO or other contact point from whom further information can be obtained;
- The likely consequences of the Personal Data Breach; and
- The measures taken or proposed to be taken to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.

If such information cannot be provided at the same time, the information may be provided in phases without undue further delay.

2.2. Communication to Individuals

OE Data Controllers must, without undue delay, inform the affected Individual of a Personal Data Breach if it is likely to result in a high risk to the Individual's rights and freedoms, describing in clear and plain language:

- The nature of the Personal Data Breach;
- The name and contact details of the OE DPP/DPO or other contact point from whom further information can be obtained;
- The likely consequences of the Personal Data Breach; and

- The measures taken or proposed to be taken to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.

OE Data Controllers do not need to provide such communication if:

- Appropriate technical and organizational protection measures have been implemented and those measures were applied to the Personal Data affected by the Personal Data Breach, particularly those that render the Personal Data unintelligible to any person who is not authorized to access it (*e.g.*, encryption);
- Subsequent measures are taken to ensure that the high risk to the Individual's rights and freedoms is unlikely to materialize; or
- It would involve disproportionate effort, in which case, a public communication or similar measure must be issued to inform affected Individuals in an equally effective manner.

2.3. Notification to the Data Controller

OE Data Processors must, without undue delay, but not later than 24 hours, on becoming aware of a Personal Data Breach, notify the Data Controller.

IX. Privacy by Design and Default

1. Privacy by Design

1.1. Global Minimum Requirements

OE Data Controllers must ensure that data privacy and protection is methodically embedded into relevant business processes and procedures and integrated into affected IT systems and applications.

1.2. Additional Requirements for EEA Processing

OE Data Controllers must implement appropriate technical and organizational measures (*e.g.*, pseudonymization) to implement data privacy and protection principles (*e.g.*, data minimization) into new products, services, and business processes and procedures, where applicable, in an effective manner, and to integrate the necessary safeguards into the Processing of Personal Data.

OE Data Controllers must implement such measures both at the time of determining the means of Processing and at the time of the Processing itself.

OE Data Controllers must consider the state of the art, cost of implementation and the nature, scope, context, and purposes of Processing, as well as the severity and likelihood of risks to the rights and freedoms of Individuals posed by the Processing.

2. Privacy by Default for EEA Processing

OE Data Controllers must implement appropriate technical and organizational measures to ensure that, by default, only Personal Data which are necessary for each specific purpose of Processing are processed. Such requirement applies to the amount of Personal Data collected, the extent of Processing, and the period of storage and access. In particular, by default, Personal Data must not be accessible to an

indefinite number of natural persons without the Individual's intervention (*e.g.*, feedback or comments submitted online should not be made public by default).

X. Cooperation with EEA data protection authorities for EEA Processing

2 OE Data Controllers and OE Data Processors must cooperate with EEA data protection authorities on the performance of their tasks.

C. Data Privacy and Protection Compliance Activities and Processes

The following compliance activities and processes are designed to facilitate adherence to the principles set out in Chapter B and to support OEs' obligations towards Individuals set out in Chapter D.

I. Privacy Impact & Ethics Assessments and Records of Processing

1 2 Where applicable, OEs must perform a Privacy Impact Assessment ("PIA"), or for Processing activities using artificial intelligence, a Privacy Impact & Ethics Assessment. As further described in the *Functional Rule for Privacy Impact & Ethics Assessments and Records of Processing*: (i) OE Data Controllers must analyze all Processing activities posing a high data privacy and protection risk against applicable legal, regulatory, and internal policy requirements and (ii) OE Data Controllers must define actions to remediate any privacy risks identified in the performance of the above activities.

Each OE Data Controller and, where applicable, the OE Data Controller's representative, must maintain a record of processing activities under its responsibility. That record shall contain all of the following information:

- The name and contact details of the OE Data Controller and, where applicable, the joint controller, the OE Data Controller's representative and the data protection officer;
- The purposes of the processing;
- A description of the categories of data subjects and of the categories of Personal Data;
- The categories of recipients to whom the Personal Data have been or will be disclosed including recipients in third countries;
- Where applicable, transfers of Personal Data to a third country, including the identification of that third country and, when required by law, the documentation of suitable safeguards;
- Where possible, the envisaged time limits for erasure of the different categories of data; and
- Where possible, a general description of the technical and organizational security measures implemented pursuant to Chapter B, Section VII. of the APS.

Each OE Data Processor and, where applicable, the OE Data Processor's representative must maintain a record of all categories of processing activities carried out on behalf of a controller, containing:

- The name and contact details of the OE Data Processor and of each controller on behalf of which the OE Data Processor is acting, and, where applicable, of the controller's or the OE Data Processor's representative, and the data protection officer;
- The categories of processing carried out on behalf of each controller;
- Where applicable, transfers of personal data to a third country, including the identification of that third country and, when required by law, the documentation of suitable safeguards; and

- Where possible, a general description of the technical and organizational security measures implemented pursuant to Chapter B, Section VII. of the APS.

II. Training

1. Global Minimum Requirements

OE Data Controllers and OE Data Processors must create and conduct periodic data privacy and protection trainings for Employees and other related persons, involved permanently or regularly in Processing Personal Data, to ensure an adequate level of knowledge and awareness.

OE Data Controllers and OE Data Processors shall have recourse to a computer-based training that is developed and maintained by Group Privacy. Participants' understanding will be tested as part of the training. OE Data Controllers and OE Data Processors must track test completion rates and performance to the extent permitted by applicable laws and regulations.

OE Data Controllers and OE Data Processors must ensure that Employees and other related persons awareness of their data privacy and protection responsibilities is maintained, for instance by using a refresher component developed by Group Privacy. The frequency and content of refresher trainings is at the discretion of the Group Chief Privacy Officer, but will be mandatory for all OEs, absent an express exemption from the Group Chief Privacy Officer.

2. Additional Requirements for EEA Processing

OE Data Controllers and OE Data Processors must provide, on a periodic basis, Employees and other related persons, involved permanently or regularly in Processing or in the development of tools used to Process EEA Personal Data, with appropriate data privacy and protection training, including on the Requirements for EEA Processing, to ensure an adequate level of knowledge and awareness.

III. Internal Requests and Complaints Mechanism

1. Global Minimum Requirements

OE Data Controllers must implement and maintain effective processes to address data privacy and protection related requests, complaints, and incidents.

2. Additional Requirements for EEA Processing

For requests from Individuals relating to their rights set out in Chapter D, OEs Data Controllers must adhere to the procedure set out in Annex D (Handling of Individuals' Requests and Complaints relating to EEA Data).

IV. Monitoring and Assurance

1. Global Minimum Requirements

OE Data Controllers and OE Data Processors, regions, and Group Privacy must perform risk-based oversight (which may include monitoring, testing, reviews, audits, and other components) of the adequate design, implementation, and effectiveness of the Framework and related processes and controls over a 5-year cycle, including by samples, surveys and reviews. OE Data Controllers and OE Data Processors must participate in data privacy and protection audits on the specific request of the GCPO.

The results must be approved by OEs' board of management, and shared – including any material deviation from the Framework, with the GCPO (and where applicable to their Regional DPP/DPO) in a timely manner.

OE Data Controllers and OE Data Processors must provide statements of accountability in connection with the Framework when requested by the GCPO.

D. Obligations towards Individuals

I. Responding to Individuals' requests to access, rectify, or erase

1. Global Minimum Requirements

OE Data Controllers must give Individuals the ability to review, correct, or delete their Personal Data, upon request and in accordance with applicable laws and regulations, provided Individuals first authenticate their identity to an appropriate level of assurance.

Where requests are denied, Individuals must be given reasons for such denial together with the right to challenge such decision.

2. Additional Requirements for EEA Processing

OE Data Controllers must adhere to the procedure set out in Annex D (Handling of Individuals' Requests and Complaints relating to EEA Data) when responding to Individuals' requests to access, rectify, and erase Personal Data.

2.1. Access request

OE Data Controllers must give Individuals the ability to access, upon request, the following:

- Confirmation of whether the Data Controller has Personal Data relating to them;
- A copy of their Personal Data;
- The purpose(s) of the Processing;
- The categories of Personal Data held about the Individual;
- The recipients or categories of recipients to whom the Personal Data are disclosed (particularly recipients in non-EEA countries) and the appropriate safeguards provided to such transfers;
- Where possible, the period for which the Personal Data will be stored, or, if not possible, the criteria used to determine that period;
- The existence of the right to request from the Data Controller rectification or erasure of Personal Data, or restriction of Processing of Personal Data concerning the Individual, or to object to such Processing;
- The right to lodge a complaint with an EEA data protection authority;
- Where the Personal Data are not collected from the Individual, any available information as to the source; and
- The existence of automated decision-making, including Profiling, referred to in Chapter D, Section V. and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such Processing for the Individual.

OE Data Controllers may reject such requests in the instances listed in Annex D, Section V. (Handling of Individuals' Requests and Complaints relating to EEA Data). Further requirements for access requests are set out in the Functional Rule for the handling of Subject Access Requests (SARs) and Data Privacy Complaints (Complaints).

2.2. Rectification request

OE Data Controllers must give Individuals the ability to request, without undue delay, rectification of their Personal Data (including by means of providing a supplementary statement considering the purpose(s) of the Processing) which does not comply with applicable EEA laws and regulations, in particular because it is incomplete or inaccurate.

OE Data Controllers may reject such requests in the instances listed in Annex D, Section V. (Handling of Individuals' Requests and Complaints relating to EEA Data).

2.3. Erasure request

OE Data Controllers must give Individuals the ability to request the erasure of their Personal Data if:

- The Personal Data are no longer necessary in relation to the purpose(s) for which they were collected or otherwise Processed;
- The Individual withdraws consent on which the Processing is based, and there is no other lawful basis for the Processing;
- The Individual objects to Processing performed on the basis of the Data Controller's legitimate interests where there are no overriding legitimate grounds for the Processing, or the Individual objects to the Processing for direct marketing purposes;
- The Personal Data have been unlawfully processed;
- The Personal Data must be erased for compliance with applicable EEA laws and regulations to which the Data Controller is subject; or
- The Personal Data relate to a child or to an Individual whose Personal Data were collected when they were a child, as defined under applicable EEA laws and regulations, in relation to the offer of information society services.

Where the Personal Data subject to the request to erasure have been made public by the Data Controller, it must take reasonable steps, including technical measures, to inform Data Controllers which are Processing the Personal Data, of the Individual's request to erase any links to, or copies of, those Personal Data.

OE Data Controllers may reject a request from an Individual to erase their Personal Data in the instances listed in Annex D, Section V. (Handling of Individuals' Requests and Complaints relating to EEA Data). In such instance, OE Data Controllers may restrict the Processing of Personal Data subject to the request to erase, if further requested by the Individual in accordance with Chapter D, Section III.

II. Responding to Individuals' requests to object to EEA Processing

OE Data Controllers must give Individuals the ability to object at any time to the Processing of their Personal Data which is based on the Data Controller's legitimate interests, including Profiling. In such case, OE Data Controllers must cease Processing of the Personal Data unless they can demonstrate compelling legitimate grounds for continuing the Processing that override the Individual's interests, rights and freedoms, or for the establishment, exercise or defense of legal claims.

OE Data Controllers must give Individuals the ability to object at any time to the Processing of their Personal Data for direct marketing purposes (including Profiling, to the extent that it is related to direct marketing). On the exercise of such right by Individuals, OE Data Controllers must cease Processing for direct marketing purposes.

OE Data Controllers must adhere to the procedure set out in Annex D (Handling of Individuals' Requests and Complaints relating to EEA Data) when responding to objection requests from an Individual. OE Data Controllers may reject such requests in the instances listed in Annex D, Section V.

III. Responding to Individuals' requests to restrict EEA Processing

2 OE Data Controllers must give Individuals the ability to restrict the Processing of their Personal Data, and to have their Personal Data segregated accordingly, if:

- The accuracy of the Personal Data is contested by the Individuals, for a period enabling the OE Data Controller to verify the accuracy of the Personal Data;
- The Processing is unlawful and the Individuals oppose the erasure of the Personal Data and request the restriction of their use instead;
- The OE Data Controller no longer needs the Personal Data for the purposes of the Processing, but they are required by the Individuals for establishing, exercising or defending legal claims; or
- The Individuals have objected to Processing carried out on the basis of the OE Data Controller's legitimate interests, pending verification of whether the legitimate grounds of the OE Data Controller override those of the Individuals.

Where the Processing is restricted, OE Data Controllers may only Process Personal Data, with the exception of storage:

- With the Individual's 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.

Where an OE Data Controller has restricted the Processing in response to an Individual's request, it must inform the Individual of such Processing restriction before it is lifted.

OE Data Controllers must adhere to the procedure set out in Annex D (Handling of Individuals' Requests and Complaints relating to EEA Data) when responding to requests for restriction from Individuals. OE Data Controllers may reject such requests in the instances listed in Annex D, Section V.

IV. Responding to Individuals' requests for portability for EEA Processing

2 Where the Processing is based on consent or on a contract and carried out by automated means, OE Data Controllers must give Individuals the ability to request to:

- Receive the Personal Data they have provided to an OE Data Controller, in a structured, commonly used and machine-readable format; and
- Transmit their Personal Data to another Data Controller without hindrance from the initial OE Data Controller, or to have such Personal Data transmitted directly from one Data Controller to another, where technically feasible.

OE Data Controllers must give effect to an Individual's request to portability of their Personal Data provided this does not adversely affect the rights and freedoms of others. An Individual's right to request portability of their Personal Data is without prejudice to the Individual's right to erasure.

OE Data Controllers must adhere to the procedure set out in Annex D (Handling of Individuals' Requests and Complaints relating to EEA Data) when responding to data portability requests from Individuals. OE Data Controllers may reject such requests in the instances listed in Annex D, Section V.

V. Responding to Individuals' requests to object to automated decisions for EEA Processing

2 OE Data Controllers must give Individuals the ability to object to any decision producing a legal effect concerning that Individual or which otherwise significantly affects that Individual that is based solely on the automated Processing of their Personal Data, including based on Profiling.

OE Data Controllers may deny such request if the decision is:

- Necessary for entering into, or for the performance of, a contract between the Individual and the OE Data Controller;
- Authorized by applicable EEA laws and regulations to which the OE Data Controller is subject and which lay down suitable measures to safeguard Individuals' rights and freedoms, and legitimate interests; or
- Based on the Individual's explicit consent.

OE Data Controllers must only make decisions based solely on the automated Processing of Individuals' Sensitive Personal Data provided they have established suitable measures to safeguard the Individual's rights, freedoms, and legitimate interests, and:

- The Individual has given their explicit consent; or
- The Processing is necessary for reasons of substantial public interest, on the basis of applicable EEA laws and regulations.

OE Data Controllers must adhere to the procedure set out in Annex D (Handling of Individuals' Requests and Complaints relating to EEA Data) when responding to Individuals' objections to decisions affecting them based on automated Processing, including Profiling. OE Data Controllers may reject such requests in the instances listed in Annex D, Section V.

E. Roles and Responsibilities

This Chapter sets forth the roles and responsibilities of persons tasked with compliance activities set forth in Chapters C and D.

I. Allianz Group Level

1. The Allianz SE Board of Management

The Allianz SE Board of Management has overall responsibility for instituting a data privacy and protection program across Allianz Group, and ensuring compliance therewith.

2. Group Privacy

The member of the Allianz SE Board of Management in charge of business division H6 has overall responsibility for Group Privacy ("GP") until January 1, 2023, at which time, overall responsibility for GP will move to the member of the Allianz SE Board of Management in change of business division H4. GP is assigned responsibility for the development, effective implementation, and maintenance of the data privacy and protection program across Allianz Group and must:

- Advise OEs on all topics related to data privacy and protection laws, regulations, regulatory guidance, as well as compliance therewith, and must support and liaise with other functions on related topics;
- Liaise with authorities, regulators, associations, and other stakeholders on matters related to data privacy and protection;
- Prepare a data privacy and protection report to be delivered annually by the Group Chief Privacy Officer to the Allianz SE Board of Management, including details of data privacy and protection maturity across the Allianz Group and any material non-compliance with the Framework;
- Monitor OEs' implementation of, and adherence to, the APS in conjunction with other relevant functions at the Allianz Group-level, or through independent reviews, including performing any necessary reviews;
- Maintain and update the APS and notify OEs and Individuals of any such changes without undue delay;

  ;and
- Liaise with OE DPPs/DPOs on the appropriate handling of Personal Data Incidents or Breaches and Individuals' exercise of their rights set out in Chapter D.

2.2 Group Privacy Interfaces with other Control Functions

GP maintains interfaces with other Allianz SE Group functions whose activities intersect with data privacy.[1]

2.2.1. Relationship with Group Risk

[1] OE data privacy functions must define analogous cooperative arrangements with local control functions which may deviate from the interfaces defined in herein based on the nature of the OE's business activities and data privacy risks arising therefrom.

Privacy risk is classified as an operational risk within Allianz Group's overall risk categorization methodology. Group Risk must define the overarching principles, processes and responsibilities for the management of operational risk via the Integrated Risk and Control System (IRCS). GP is responsible for defining the privacy risks and controls within the IRCS framework.

Any additional risk-related procedures to assess data privacy risks, if any, must be aligned between GP and Group Risk.

2.2.2. Relationship with Group Compliance

Group Compliance is responsible for defining principles, processes, and tools for the annual OE self-assessment: the Compliance Assessment of Risks and Effectiveness. GP is responsible for outlining the specific content for data privacy and performs related activities, including expert challenges. Group Compliance and GP must align on performing joint monitoring activities, such as joint reviews of OE, whenever possible.

As concerns data privacy complaints or Personal Data Incidents reported through Group Compliance channels, including CCMT, Group Compliance must inform GP to ensure timely handling of each case. GP must make reciprocal notifications of such complaints to Group Compliance.

2.2.3. Relationship with Group Information Security

Group Information Security (GIS) steers and oversees the Information Security Management System (ISMS), which comprises the rules and guidelines, the procedural framework as well as the supporting organizational setup for information security, as well as (i) defines the information security requirements; (ii) defines the ISMS key processes; (iii) defines the information security KPIs and respective controls; and (iv) establishes and communicates responsibilities of key information security personnel, as well as other stakeholders with responsibilities for information security.

The GP and GIS cooperate to protect the confidentiality, availability and integrity of Personal Data and to protect against improper Processing of Personal Data, and toward this end, undertake the following responsibilities:

i. Requirements for the identification, protection, and treatment of Personal Data including requirements concerning the initiation of privacy impact assessments are defined by GP;
ii. Requirements for the proper encryption and other technical means to protect information classified as confidential are defined by the GIS (cf. AFRIS Chapter E & Annex B);
iii. Requirements for information classification are defined by GIS (cf. AFRIS Chapter D and Annex B) and with respect to Personal Data, aligned with GP;
iv. The Information Security Incident Handling process requires the involvement by GP whenever Personal Data is or may be affected, and the Personal Data Incident Management process requires the involvement of GIS when corporate data – beyond Personal Data – is or may be affected;
v. GIS and GP align on the performance of joint monitoring activities, whether event-related or for control effectiveness (*e.g.*, peer reviews), and the results from such monitoring activities will be shared between the two functions; and
vi. GIS and GP align on a consolidated and unified management reporting process for significant cases with cross functional dimension.

2.2.4. Relationship with Group Operations & Performance

Group Operations & Performance (GOP) has responsibility for promoting and facilitating privacy by design for areas under the mandate of GOP, which may include designing processes, common solutions and managing operations.[2] GP is responsible for advising and monitoring compliance with data protection laws and the Allianz privacy framework, including as pertains to GOP activities.

GP and GOP are required to liaise on matters affecting privacy compliance across Allianz Group, including with respect to GOP-driven projects or initiatives with privacy implications and regulatory change projects.

GP and GOP (Protection & Resilience) cooperate in performance of monitoring activities including self-assessments and joint reviews, and support consolidated and unified management reporting. In addition, GP is part of the extended crisis unit and collaborates with P&R to participate in Crisis Scenario Plans and training exercises.

GP and GOP (Procurement) are required to align on the sound implementation of Privacy controls in the Procurement framework, including pre-contractual supplier due diligence activities, data processing agreements, and ongoing periodic supplier monitoring activities.

2.2.5. Relationship with the Group Legal

GP and Group Legal (GL) cooperate on the interpretation of Privacy regulations, statutes, and other sources of law applicable to Allianz Group. GL is responsible for providing legal advice on contractual topics, in particular data processing agreements and EU Data Transfer Model Clauses, and GP is responsible for ensuring the related Annexes to these agreements (e.g., affected data categories and technical and organizational measures) are completed accurately. GL is also the owner of the ASIDM. With respect to this standard, GP is responsible for determining the retention period for Non-Relevant Documents and is collaborating with Group Legal on retention periods for Relevant Documents.

GP retains responsibility for data protection legal matters that are not contractual in nature context including, *inter alia*, the Allianz Privacy Framework, managing regulatory change projects, and addressing data privacy requirements in personal data processing activities.

6. Relationship with the Group Audit

Given the nature of their respective responsibilities, GP and GAUD are separate functions with no lines of reporting in either direction. Nonetheless, GP and GAUD are permitted to jointly exercise specific responsibilities in the course of investigations.

The data privacy topic is included in the Master Audit Universe developed by GAUD, and GAUD will undertake a periodic assessment of the adequacy and effectiveness of GP controls and processes. Based on the annual audit plan and scope, GP is permitted to rely on audit procedures performed by GAUD. In addition, GAUD is

[2] Notwithstanding the responsibilities of GOP, business owners retain obligation of complying with the Allianz Privacy Framework.

required to keep GP informed of data privacy audit findings arising out of practice audits of Allianz OEs.

3. Group Chief Privacy Officer

The Group Chief Privacy Officer ("GCPO") is the head of Group Privacy of the Allianz Group. The GCPO is appointed by the Allianz SE Board of Management board member in charge of GP.

The GCPO must:

- Report directly to the member of the Allianz SE Board of Management with responsibility for GP;
- Be involved, properly and in a timely manner, in all issues relating to data privacy and protection;
- Have appropriate resources and unfettered access to Processing activities;
- Maintain their expert knowledge;
- Act independently (*i.e.*, not receive any instructions) regarding the exercise of their tasks;
- Be protected from dismissal or penalty in performing their tasks;
- Be bound by secrecy or confidentiality concerning the performance of their tasks, in accordance with applicable EEA laws and regulations;
- Perform any other tasks and duties provided they do not result in a conflict of interest (*e.g.*, the GCPO must not hold a position that leads them to determine the purposes and means of the Processing of Personal Data);
- Publish their contact details and communicate them to Allianz's lead data protection authority, the Bavarian data protection authority (BayLDA), and notify it of any changes thereafter; and
- Be accessible to Individuals on all issues related to the Processing of their Personal Data and the exercise of their rights.

The GCPO is responsible for overseeing Group Privacy's effective implementation and maintenance of data privacy and protection throughout the Allianz Group and must:

- Advise and train the Allianz SE Board of Management on all topics related to data privacy and protection laws, regulations, and regulatory guidance, as well as compliance therewith;
- Advise and train Employees and other staff on their obligations and rights under the APS;
- Prepare and implement Group-wide data privacy and protection initiatives;
- Monitor compliance with applicable data privacy and protection laws, regulations, regulatory guidance, and the Framework across Allianz Group;
- Liaise with other functions at the Allianz Group-level on the appropriate handling of Personal Data Incidents or Breaches and on Individuals' exercise of their rights set out in Chapter D;

- Adhere to the procedure for requests and complaints from Individuals set out in Annex D (Handling of Individuals' Requests and Complaints relating to EEA Data), when complaints are escalated to them;
- Deliver an annual data privacy and protection report to the Allianz SE Board of Management, including details of data privacy and protection maturity across the Allianz Group and any material non-compliance with the Framework;
- Act as the point of contact for, and cooperate with, EEA data protection authorities for any request related to EEA Processing performed at Group level, including prior consultation on PIAs;
- In line with the *Allianz Governance and Control Policy*: (i) Nominations of Regional DPOs and OE DPOs/DPPs shall be pre-aligned with the GCPO; and (ii) the GCPO annually may propose a Group-related target for the Regional DPOs and the OE DPOs/DPPs and shall be involved in the respective assessment process.
- For OEs without a Regional DPO, act cooperatively with OEs board of management to:
    - Create and maintain a network of DPPs/DPOs in the Allianz Group;
    - Establish functional reporting lines from DPPs/DPOs to the GCPO;
    - Set functional targets for DPPs/DPOs with respect to data privacy and protection activities;
    - Provide verbal and written evaluations of DPPs/DPOs performance;
    - Propose compensation and bonus levels of DDPs/DPOs; and
    - Make recommendations concerning discipline or termination of DPPs/DPOs.
- Install and maintain the Allianz Privacy Advisory Group ("APAG");
- At their discretion, waive in whole or in part any Global Minimum Requirement for any non-EEA OE Data Controller or Data Processor for which the Requirements for EEA Processing are inapplicable. The GCPO must document in writing any exception to the Global Minimum Requirements and the reasoning supporting this decision;
- Liaise with OEs' DPPs/DPOs and other relevant stakeholders to:
    - Resolve any conflict between the provisions of the APS and local laws and regulations; and
    - Report any issue to the competent EEA data protection authorities arising from laws and regulations applicable to a non-EEA OE which are likely to have a substantial adverse effect on the guarantees provided in the APS, including, to the extent permitted, any legally binding request for disclosure of EEA Data by a law enforcement authority or state security body; and
- Advocate the Allianz Group's data privacy and protection interests with authorities, regulators, associations, and other stakeholders.

The GCPO also acts as the OE Data Protection Officer ("DPO") for Allianz SE and for this purpose has a direct functional reporting line to the member of the Allianz SE Board of Management with responsibility for GP. In the performance of their responsibilities, the GCPO must have due regard to the risks associated with Processing undertaken by Allianz SE considering the nature, scope, context, and purpose(s) of the Processing.

II. Allianz Regional Level

Regions must designate a Regional DPO. The Regional DPOs are responsible for managing and monitoring the effective implementation and maintenance of data privacy and protection in their Region, as well as compliance with applicable data privacy and protection laws and the Privacy Framework, and informing and advising the Employees in their Region of their data protection obligations.

The appropriate allocation of resources for the Regional DPO is based on the activities to be performed and the capabilities needed by the privacy function, as well as the nature of the business, the complexity of its operations, and the regulatory environment in which it operates. In circumstances where an individual performs roles in addition to that of Regional DPO that could lead to a conflict of interest, the proportion of time that the individual dedicates to executing the responsibilities of the Regional DPO must be documented.

The Regional DPO must:

i. Oversee the appropriate implementation of the Privacy Framework by OEs within the region, and monitor, through regional monitoring activities (*e.g.*, annual program maturity assessment and reviews), that privacy compliance processes are appropriately implemented, maintained, and adhered to in accordance with respective internal and external requirements;
ii. Align and report to GP, the results of monitoring activities, in particular, the existence of privacy issues or audit findings, and coordinate the timely remediation of the same;
iii. Advise DPOs/DPPs within the region on their obligations under the Privacy Framework, including facilitating privacy training;
iv. Promptly inform GP of material regulatory investigations/actions and cooperate with the local DPOs/DPP to handle the same;
v. Support, where applicable, local DPOs/DPPs cooperation with competent data protection authorities on privacy-related issues;
vi. Conduct, at a minimum, quarterly calls with local DPOs/DPPs under their responsibility; and
vii. Participate in the Allianz Privacy Advisory Group (“APAG”) upon request of the GCPO.

III. Allianz OE Level

1. OE Board of Management

1.1. Global Responsibilities

The OE board of management is responsible for establishing and maintaining a sound and clearly defined organizational and operational set-up to ensure compliance with the Framework, and must:

- Ensure adequate resource, staff training, record-keeping, data quality, and IT systems and monitoring;
- Ensure adequate resource for compliance with the procedure for the exercise of Individuals’ rights set out in Annex D (Handling of Individuals’ Requests and Complaints relating to EEA Data);
- Where required under applicable laws and regulations, appoint, and obtain the pre-approval of the GCPO for, a Data Protection Officer (“DPO”) either as a

dedicated position or as a defined responsibility within an existing function (*e.g.*, OE legal or compliance function) that:

- Meets the requirements of applicable laws and regulations;
- Has the necessary qualifications and expertise to fulfill the role of a DPO for example, sufficient understanding of the Processing operations carried out, as well as the information systems, security, and privacy and data protection needs of the OE, including the duties set out in Section 2 below;
- Has a functional and administrative reporting line to the OE board member responsible for data privacy and protection;
- Can act independently, with unfettered access to Processing activities and information, and without any conflict of interest (*i.e.*, the DPO must not hold a position that leads them to determine the purposes and means of the Processing of Personal Data); and
- Will participate in the Allianz Privacy Advisory Group ("APAG") upon the request of the GCPO;

- Appoint a Data Privacy Professional ("DPP") where applicable laws and regulations do not require the appointment of a DPO and ensure that they are provided with appropriate support and resources to fulfill their tasks and duties. Such DPP:
  - Must be appropriately qualified to fulfill the duties set out in Section 2 below; and
  - Will participate in the APAG upon the request of the GCPO;
- Act cooperatively with the GCPO or the Regional DPO, as applicable, to:
  - Pre-align on the appointment of a DPP/DPO;
  - Establish functional reporting lines from the DPP/DPO to the GCPO;
  - Set functional targets for the DPP/DPO with respect to data privacy and protection activities;
  - Act on any verbal or written evaluations made by the GCPO or the Regional DPO, as applicable, of the DPP/DPO's performance;
  - Set compensation and bonus levels of the DDP/DPO; and
  - Discipline or terminate the DPP/DPO.

2 1.2. Additional Responsibilities for EEA Processing

The OE board of management must designate an OE Data Protection Officer ("DPO") where:

- The OE's core activities, acting either as a Data Controller or as a Data Processor, consist of Processing which, by its nature, scope and/or purpose(s), requires regular and systematic monitoring of Individuals (*e.g.*, email retargeting; data-driven marketing activities; Profiling and scoring for purposes of risk assessment (*e.g.*, credit scoring, establishment of insurance premiums, fraud prevention, detection of money-laundering); location tracking; behavioural advertising; monitoring of wellness, fitness, and health data via wearable devices; connected devices (*e.g.*, smart meters, smart cars, home automation) on a large scale (*e.g.*, Processing of customer Personal Data for the establishment of insurance premiums);

- The OE's core activities, acting either as a Data Controller or as a Data Processor, consist of Processing on a large scale of Sensitive Personal Data, and Personal Data relating to criminal convictions and offences (cf. Chapter B, Sections IV.2-2.2. and 2.3.); or
- This is required by applicable laws and regulations.

When assessing if a DPO must be designated as described above, the OE board of management must document such assessment in order to demonstrate that the relevant factors have been properly considered. Such assessment should be re-performed where necessary (*e.g.*, if the OE undertakes new activities or provides new services that could meet the above criteria).

The OE board of management must ensure that the DPO:

- Is appointed in accordance with applicable EEA laws and regulations and/or the requirements of EEA data protection authorities from time to time;
- Has direct functional and administrative reporting lines to the OE board of management;
- Is involved, properly and in a timely manner, in all issues relating to data privacy and protection, *i.e.*, the DPO must be included as a discussion partner for matters relating to Processing activities and their opinion given due weight. Any deviation from their advice must be documented;
- Has appropriate resources, unfettered access to Processing activities, and maintains their expert knowledge;
- Acts independently (does not receive any instructions) regarding the exercise of those tasks;
- Is protected from dismissal or penalty in performing their tasks;
- Is bound by secrecy or confidentiality concerning the performance of their tasks, in accordance with applicable EEA laws and regulations;
- Performs any other tasks and duties provided they do not result in a conflict of interest (*e.g.*, the DPO must not hold a position within the OE that leads them to determine the purposes and means of the Processing of Personal Data);
- Publish their contact details, communicate their name and contact details to the EEA data protection authority competent for the OE, and notify such data protection authority of any changes thereafter; and
- Be accessible to Individuals (e.g., being located in the EU, where appropriate) on all issues related to the Processing of their Personal Data and the exercise of their rights.

2. OE Data Privacy Professional/Data Protection Officer

2.1 Appropriate Resources

The appropriate resources for the OE DPO/DPP is based on the activities to be performed and the capabilities needed by the privacy function, as well as the nature of the business, the complexity of its operations, and the regulatory environment in which it operates.

In circumstances where an individual performs roles in addition to that of DPO/DPP that could lead to conflict of interest, the proportion of time that the individual dedicates to executing the responsibilities of the DPO/DPP must be documented.

As concerns Allianz SE Solo, in case of conflicts of interest between the role of the DPO of AZ SE and the GCPO, the GCPO must refer the matter to the AZ SE Board of Member responsible for Privacy for advice and resolution, and whose determination is final and binding on the GCPO.

2.2 Global Responsibilities

The OE Data Privacy Professional ("DPP") / Data Protection Officer ("DPO") must:

- Ensure appropriate implementation of the Framework at OE level;
- Align their functional activities with targets and directives set jointly by the OE board of management and GCPO;
- Monitor compliance with applicable data privacy and protection laws, regulations, regulatory guidance, and the Framework in the OE;
- Validate that data privacy and protection-related compliance processes are appropriately implemented, maintained, and adhered to in accordance with respective internal and external requirements;
- At the direction of the GCPO, report the results of monitoring activities, in particular, the existence of material OE data privacy and protection deficiencies;
- Advise Employees on their obligations and rights under the Framework, including through conducting or facilitating training, awareness, and communication on data privacy and protection;
- Have due regard, in the performance of their responsibilities, to the risk associated with Processing, considering the nature, scope, context, and purpose(s) of the Processing;
- Perform the tasks and duties set out in Section III.3. below, unless they decide to delegate some of them to the OE Privacy Champion(s), in which case the OE DPP/DPO retains the responsibility for overseeing the Privacy Champion's activities;
- Draft and retain a record of the tasks and duties they assigned to the OE Privacy Champion(s);
- Where relevant, promptly inform GP (or facilitate notification to GP via the regional privacy function, where applicable) of any confirmed or potentially material Personal Data Incident, in accordance with the reporting requirements set forth in the Functional Rule for Personal Data Incident Management;
- Liaise with the GCPO or GP to:
    - Resolve any conflicts between the provisions of the APS and local laws and regulations;
    - Report any issue to the competent data protection authorities arising from laws and regulations applicable to a non-EEA OE which are likely to have a substantial adverse effect on the guarantees provided in the APS, including, to the extent permitted, any legally binding request for disclosure of EEA Data by a law enforcement authority or state security body;
    - Clarify the scope or application of any part of the Framework;
- Liaise with local data protection authorities, regulators, and authorities; and

- Cooperate with the GCPO and/or other OEs to handle a request or complaint from an Individual, or in response to an investigation or inquiry by any data protection authority.

Any arrangement between an OE and a third-party or Allianz Group company by which that third-party or Allianz Group company performs any of the DPP/DPO responsibilities that qualifies as Outsourcing within the meaning of the Allianz Group Outsourcing Policy (or locally-implemented equivalent thereof), is subject to the requirements of the Allianz Group Outsourcing Policy or respective local Outsourcing Policy.

2

2.3 Additional Responsibilities for EEA Processing

The OE DPP/DPO must:

- In the event of a Personal Data Breach, comply with applicable legal and regulatory requirements as well as the requirements contained in the *Functional Rule for Personal Data Incident Management,* the *Allianz Standard for Protection & Resilience* (AZ P&R Standard), the *Allianz Functional Rule for Protection & Resilience* (AZ P&R Functional Rule), the Allianz Group Information Security Framework, and any other applicable Allianz policies;

- Assess any judgment or decision taken by a non-EEA court, tribunal, or administrative authority, requiring the transfer or disclosure of EEA Data, and consult the OE or an external legal counsel, to ensure such transfer or disclosure is done in compliance with applicable EEA laws and regulations;
- In case of a legally binding request for the disclosure of EEA Data by a law enforcement authority or state security body:
    - Liaise with the GCPO or GP as soon as the OE is aware that a law enforcement authority or state security body is considering requesting disclosure of EEA Data;
    - To the extent permitted, place the request on hold for a reasonable period prior to any disclosure to the requesting authority or body in order to report it to the competent EEA data protection authorities. The information provided to the competent EEA data protection authorities should include information on the EEA Data requested, the requesting authority or body, and the legal basis for the disclosure;
    - Where the request cannot be suspended or notification to the competent EEA data protection authorities is prohibited, use and demonstrate best efforts to obtain the right to waive such prohibition in order to communicate as much information as possible to the competent EEA data protection authorities, as soon as is practicable;
    - Where waiver of the prohibition is not permitted or permission to notify the competent EEA data protection authorities is not obtained, annually provide the competent data protection authorities with general information on any requests received (*e.g.*, number of applications for disclosure, type of EEA Data requested, details of the requester, if possible, etc.); and
    - Not make any transfers of EEA Data to any requesting law enforcement authority or state security body which are massive, disproportionate and

indiscriminate in a manner that go beyond what is necessary in a democratic society;

- Cooperate with, and act as the point of contact for, competent EEA data protection authorities on issues relating to EEA Processing performed at the OE level, including prior consultation on PIAs.

3. OE Privacy Champions

1 2 OE Data Controllers and OE Data Processors, in cooperation with the OE DPP/DPO, must appoint, from within their business functions, one or more Privacy Champion(s), as is appropriate based on criteria provided by GP. A Privacy Champion is a defined responsibility within a business function, which requires the dedication of a portion of the Employee's time to assist colleagues in their business unit with privacy topics. OE Data Controllers and OE Data Processors must ensure that the Privacy Champions are provided with the support and resources necessary to fulfil their assigned tasks and duties.

3.1 Global Responsibilities

The OE Privacy Champion shall act as the communication channel between the OE business functions and the OE DPP/DPO, and unless otherwise instructed by the OE DPP/DPO, must:

- Ensure appropriate implementation of the Framework across the OE at the direction of the OE DPP/DPO;
- Support the implementation, maintenance, and adherence of data privacy and protection-related compliance processes, in accordance with the Framework;
- Support the OE on complying with data privacy and protection requirements, and timely seek the advice of the OE DPP/DPO where appropriate;
- Promote and deliver key data privacy and protection messages, and assist the OE DPP/DPO with the preparation and delivery of data privacy and protection training, awareness, and communication initiatives;
- Create and maintain logs of current, open, and resolved data privacy and protection-related requests and complaints from Individuals, queries from internal and external stakeholders, and issues and actions taken; and make such logs available to the OE DPP/DPO upon request;
- Coordinate the reporting of Personal Data Breaches to the OE DPP/DPO;
- Advise the OE business functions and the OE DPP/DPO on whether PIAs should be completed for processes or procedures that pose a low or medium privacy and data protection risk;
- Assist the OE business functions to create and maintain records of Processing activities, based on the information provided by the Information Owner and in accordance with the Functional Rule on Privacy Impact Assessments (PIAs) and Records of Processing; and
- Cooperate with the OE DPP/DPO, the GCPO, other OEs or the Regional DPO, as applicable, to handle a request or complaint from an Individual, or in response to an investigation or inquiry from any data protection authority.

3.2 Additional Responsibilities for EEA Processing

The OE Privacy Champion, unless such tasks are assigned to a separate business function under local OE policies, must:

- Independently handle requests from Individuals relating to their rights set out in Chapter D; and
- Promptly inform the OE DPP/DPO of the outcome of requests and complaints from Individuals.

4. OE Information Owner

The ownership of Personal Data for purposes of the Framework attaches to the organizational unit which has professional and business responsibility for a specific Data Processing Activity. The organizational unit that collects, or initiates the collection or storage of, Personal Data constitutes the owner of that Personal Data and is represented by the individual within the business ultimately responsible for the Processing Activity ("Information Owner"). The Information Owner must, to the extent that it relates to the Information Owner's sphere of responsibility:

- Ensure compliance with the requirements of the Framework;
- Ensure that Personal Data are collected and Processed only so far as is required to fulfill a specified, explicit, and legitimate business purpose;
- Ensure that functional responsibility of ownership of Personal Data is clearly assigned and documented and that such Personal Data is adequately identified and classified accordingly to the Allianz Group Information Security Framework (GISF); and
- Ensure that adequate and specified data privacy and protection controls are defined and applied during the lifecycle of the Personal Data (covering its collection or creation, storage, Processing, transfer, and disposal), and review those controls regularly for appropriateness and effectiveness in compliance with Allianz Group Information Security Framework (GISF).

IV. Privacy Monitoring and Assurance Framework

GP maintains a Privacy Monitoring and Assurance Program, which is executed regularly by Group/Regional/OE Privacy functions to monitor whether the design, implementation, and effectiveness of the Privacy Framework is adequate and in place.

1. Privacy Controls

i. GP defines data privacy controls, which are incorporated into the Integrated Risk and Control System (IRCS) and aligned with Group Risk. The IRCS controls for data privacy are mandatory for all OEs;

ii. OEs conduct self-assessments based on the corresponding control system (*e.g.*, the annual Compliance Assessment of Risks and Effectiveness);

iii. GP and Regional DPOs conduct independent reviews to assess the privacy compliance of OEs; and

iv. OE DPOs/DPPs must perform monitoring / control testing activities (*e.g.*, spot-checks and reviews) of legal entities / departments in scope for the OE.

2. Independent reviews

1 2 At intervals of no more than five years, the effectiveness of the control framework, as well as the information provided via the self-assessments of the OEs is subject to an independent review, which will be conducted by GP and/or Regional DPOs. GP is required to use a risk-based methodology to determine the most effective and efficient approach to selecting OEs for review.

All privacy issues identified during the independent reviews are monitored in the Compliance Issue Management Tool until remediated. Escalation to Allianz SE management may occur when issues are not remediated within the related timelines.

Observations and learnings deriving from reviews are used by OEs to continuously improve privacy compliance.

3. Quarterly reporting

1 2 GP maintains a reporting program to obtain the information deemed necessary for the purpose of monitoring OEs' privacy compliance. The reporting program allows GP to:

i. Meet Allianz regulatory requirements;

ii. Respond to requests from the Allianz SE and OE boards of management for updates on privacy matters;

iii. Fulfil its oversight obligations; and

iv. Adopt a risk-based approach to plan Group and OE activities (*e.g.*, reviews).

Each OE DPO/DPP must:

i. Implement appropriate assurance measures to ensure that only accurate and reliable information on the OE and its legal entities is consolidated and reported to GP. The information provided must be supported by adequate evidence; and

ii. Assign a point of contact to manage the reporting requirements.

V. Allianz Group and OE Steering

1. Allianz Privacy Advisory Group

1 2 OEs (including each Global Line) and Regions must be represented in the Allianz Privacy Advisory Group ("APAG"). The purpose and composition of the APAG is further described in the Allianz Privacy Advisory Group (APAG) Terms of Reference as amended from time to time.

2. Allianz Data Privacy and Protection Community

OEs DPPs/DPOs and Privacy Champions form part of the global Allianz Data Privacy and Protection community. The Data Privacy and Protection community is led and coordinated by GP in order to ensure comprehensive Data Privacy and Protection coverage across the Allianz Group.

F. References

The APS forms part of the Allianz Data Privacy and Protection Framework ("Framework"). The Framework includes the following as amended from time to time:

- Functional Rule for Privacy Impact & Ethics Assessments and Records of Processing
- Functional Rule for the handling of Subject Access Requests (SARs) and Data Privacy Complaints
- Functional Rule for Personal Data Incident Management

In addition, the Framework is supplemented by the following as amended from time to time:

- Allianz Binding Corporate Rules (BCRs)
- Allianz Group Information Security Framework (GISF), comprised of:
  - Allianz Group Information Technology and Information Security Policy (APITIS)
  - Allianz Functional Rule for Information Security (AFRIS)
  - Allianz Functional Rule for Information Risk Management (AFIRM)
  - Allianz Information Security Practices
- Allianz Standard for Information and Document Management (ASIDM)
- Allianz Standard for Protection & Resilience (AZ P&R Standard)
- Allianz Functional Rule for Protection & Resilience (AZ P&R Functional Rule)

Further information is available via Allianz Connect in the Corporate Rule Book.

Annex A: Glossary [1] [2]

Term	Description
Allianz Group	Allianz SE and its subsidiaries (cf. Annual Report, Glossary, term 'affiliated enterprises'), excluding associated enterprises, joint ventures (unless Group Privacy has made a formal determination of applicability as to such entity or as expressly stated in the joint venture agreement) and holding companies without operational or strategic function, but including Sub-Groups (i.e. organizational unit for a business segment or business within a region that is organized with a separate holding company controlling the subsidiaries and setting standards for them) and organizational units like Allianz Re.
APAG	The Allianz Privacy Advisory Group, a counseling and steering body established to support the furtherance of a sustainable level of data privacy and protection within the Allianz Group through the development and implementation of data privacy and protection activities, projects and initiatives.
Competent Supervisory Authority	The Supervisory Authority in the Member State of an Individual's habitual residence, place of work, or place of the alleged infringement if the Individual considers that the processing of personal data relating to him or her infringes the General Data Protection Regulation.
Data Controller	A natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes ("why") and means ("how") of the Processing of Personal Data. In the event that two or more Data Controllers jointly determine the purposes and means of Processing, they shall be considered joint controllers and must cooperate in a transparent manner to ensure adherence to the Framework.
Data Processor	A natural or legal person which Processes Personal Data on behalf of a Data Controller.
EEA	The countries forming part of the European Union from time to time, as well as Iceland, Liechtenstein, and Norway.
EEA Data	Personal Data, the Processing of which is subject to EEA laws and regulations.
EEA Processing	The Processing of EEA Data where: ▪ Personal Data are Processed in the context of the activities of a Data Controller or Data Processor's establishment in the EEA, even if the Processing itself does not take place in the EEA; or ▪ Personal Data of Individuals who are in the EEA are Processed for the offering of goods or services to Individuals, or for the monitoring of their behavior.
Employees	An OE's employees (including any full-time, part-time, interim and casual workers; consultants, contractors, and temporary workers; interns and work experience students), managers, directors and executive board members.

Framework	The *Allianz Privacy Standard* ("APS") and its Functional Rules listed in Chapter F. References.
Global Line	Lines of business that are run globally not locally or regionally, *i.e.*, AGCS, Allianz Partners, Allianz Trade, and Allianz Technology.
Group Chief Privacy Officer or GCPO	The head of Group Privacy of the Allianz Group, appointed by the Allianz SE Board of Management.
Group Privacy or GP	The Group Privacy department at Allianz SE.
Individual	An identified or identifiable natural person to whom Personal Data relates. An identifiable natural person is one who can be identified, directly or indirectly, in particular 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 Framework, it refers to Employees and related staff, customers, business partners, or any other third-parties whose Personal Data are Processed, as further described in Annex B.
Information Owner	The business person, which may include a Document Owner as defined in the ASIDM or a Business Owner of a Business Application as defined in the AFRIS, ultimately responsible for the Personal Data Processing Activity within the organizational unit that creates, or initiates the creation or storage of Personal Data.
Intra-Company Agreement or ICA	The Intra-Company Agreement for the implementation of Allianz' BCRs, signed by legal entities within the Allianz Group in order to give legal effect to the BCRs.
OE	A management entity within a business segment irrespective of its legal form (and which is under Allianz's control according to German Stock Corporation Law), excluding associated enterprises and joint ventures (unless Group Privacy has made a formal determination of applicability as to such entity or as expressly stated in the joint venture agreement). An OE can consist of one or more legal entities, or, vice versa, one legal entity may comprise of two OEs (e.g., in case of composites). Reference to an OE include a reference to all legal entities and branches that form part of this OE.
Privacy Champions	The persons with defined responsibility within existing OE business functions who act as the communication channel between OE business functions and the OE DPPs/DPOs, and supports the OE business function with privacy related topics and data protection compliance as instructed by the OE DPP/DPO or as delegated by the Information Owner.
Personal Data	Any information relating to an Individual.
Personal Data Breach	Means a breach of security leading to the accidental or unlawful destruction, loss, alteration, compromise, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed by or on behalf of Allianz, and which triggers regulatory obligations.
Personal Data Incident	An event that involves, or could involve Personal Data and which has the potential to become a Personal Data Breach. For the

	purpose of the APS, Personal Data Incident may also refer to potential Personal Data Breach.
Privacy Impact & Ethics Assessment or PIA	A structured and repeatable analysis of initiatives and existing or planned changes affecting business processes, procedures, systems, products, or services involving the Processing of Personal Data. This analysis provides information to identify, evaluate and mitigate data privacy and protection risks, including those arising from the use of Artificial Intelligence in Personal Data Processing Activities, and describes adequate and proportionate measures to reduce the impact and likelihood of data privacy and protection risks including technical and organizational measures (e.g. regulations, procedures, guidelines, legal contracts, management practices, or organizational structures).
Processing	Any operation or set of operations performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.
Profiling	Any form of automated processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to an Individual, in particular to analyse or predict aspects concerning that Individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location, or movements.
Regions	Regions include Asia Pacific (APAC), Central and Eastern Europe (CEE), and Iberia & Latin America (IberioLatAm).
Representative	A natural or legal person established in the European Union who, designated the OE Data Controller or OE Data Processor in writing, represents the OE Data Controller or Data Processor with regard to their respective data privacy obligations.
Subject Access Requests or SARs	The exercise, by Individuals, of their access request right relating to the Processing of their Personal Data, as provided by applicable laws and regulations, and covered in Chapter D, Section I, 2.1.
Sensitive Personal Data	Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the Processing of genetic data, biometric data for the purpose of uniquely identifying an Individual, data concerning health or data concerning an Individual's sex life or sexual orientation. Personal Data which by its nature could potentially pose a higher risk to the privacy and data protection rights and freedoms of an Individual but is not included here is known as "Other Sensitive Personal Data" (*e.g.*, bank account details, salary, identity document details, signatures). Sensitive Personal Data and Other Sensitive Personal Data require a higher level of protection than Personal Data (*e.g.*, consent, encryption).
Supervisory Authority	Is an independent public authority which is established by an EU member state to be responsible for monitoring the application of this General Data Protection Regulation.

Annex B: Minimum Requirements for Data Controller - Data Processor Contractual Relationships for EEA Processing [2]

I. Non-OE Data Processors

For EEA Processing, OE Data Controllers must incorporate the following requirements when contracting with non-OE Data Processors, pursuant to Chapter B, Section V.2.

Provisions relating to the EEA Processing:

- ✓ Subject-matter and duration of the Processing;
- ✓ Nature and purpose of the Processing; and
- ✓ Type of Personal Data and categories of Individuals

Obligations and rights of the OE Data Controller:

- ✓ Obligations of the OE Data Controller; and
- ✓ Rights of the OE Data Controller

Data Processor commitments:

- ✓ Process Personal Data only on documented instructions from the OE Data Controller, including for transfers to non-EEA countries;
- ✓ Report on any EEA laws and regulations applicable to the Data Processor which require it to Process the Personal Data beyond the scope of the OE Data Controller's instructions, unless such information is prohibited on important grounds of public interest;
- ✓ Ensure that authorizations to Process Personal Data have only been granted to persons bound by a confidentiality commitment or an appropriate statutory obligation of confidentiality;
- ✓ Take all necessary security measures such that the Processing will meet the requirements set out in Chapter B, Section VII.2.;
- ✓ Engage sub-Processors only with the OE Data Controller's prior specific or general written authorization;
- ✓ If a general written authorization is given by the OE Data Controller, inform the OE Data Controller of any intended changes concerning the addition or replacement of sub-Processors together with the opportunity to object to such changes;
- ✓ Transfer its data privacy and protection obligations to sub-Processors by way of a contract or other legal act, without discharging itself from its liability to the OE Data Controller, including for any breach or failure by the sub-Processors;
- ✓ Assist the OE Data Controller by appropriate technical and organizational measures taking into account the nature of the Processing and insofar as this is possible, for the fulfilment of the OE Data Controller's obligation to respond to requests for exercising Individuals' rights;

- ✓ Assist the OE Data Controller in ensuring compliance with its obligations relating to security, notification of Personal Data Breaches to EEA data protection authorities and/or Individuals, and PIAs, taking into account the nature of Processing and the information available to the Data Processor;
- ✓ At the choice of the OE Data Controller, delete or return all Personal Data to the OE Data Controller at the end of the provision of any services relating to Processing, and delete existing copies unless applicable EEA laws and regulations require storage of the Personal Data; and
- ✓ Make available to the OE Data Controller all information necessary to demonstrate compliance with its obligations under applicable EEA laws and regulations and allow for and contribute to audits, including inspections, conducted by the OE Data Controller or another auditor mandated by the OE Data Controller; and immediately inform the OE Data Controller if, in its opinion, an instruction infringes applicable EEA laws and regulations.

II. OE Data Processors

By default, the APS requirements apply to both OEs acting as Data Controllers and OEs acting as Data Processors on-behalf of OE Data Controllers, unless stated otherwise. Besides, where Requirements for EEA Processing apply only to OE Data Controllers, OE Data Processors must adhere to the standards imposed on those OE Data Controllers, and facilitate the OE Data Controllers' ability to comply with such standards.

Moreover, the conditions in connection with EEA Processing, pursuant to Chapter B, Section V.2 of the APS, apply.

Annex C: Handling of Individuals' Requests and Complaints relating to EEA Data [2]

The procedure set out in this Annex D applies to EEA Data in respect of requests and complaints from Individuals pursuant to Chapter D, Sections I. to V. and complaints from individuals pursuant to Chapter C, Section III.

OE Data Controllers must adhere to the procedure described below in order to facilitate the exercise of an Individual's right to:

- Access, rectification, erasure, objection, restriction, portability, and the rights relating to automated individual decisions (including Profiling); and
- Complain about any issue relating to the Requirements for EEA Processing under which their Personal Data are processed.

The Privacy Champion or DPP/DPO of the OE Data Controller at the origin of the Processing, as appropriate, shall be responsible for handling such requests and complaints.

I. Confirmation of an Individual's identity

Where the applicable Privacy Champion or DPP/DPO of the OE Data Controller, as appropriate, has any reasonable doubt concerning the identity of an Individual making the request or complaint, or where required by applicable EEA laws and regulations, they may request additional information in order to confirm the identity of the Individual, except if the request or complaint relates to automated decisions (including Profiling).

II. Process and timelines to handle requests and complaints

The following steps outline the process to be undertaken by the Privacy Champion or DPP/DPO of the OE Data Controller when handling requests and complaints of Individuals:

Step 1

- Acknowledge receipt of the Individual's request or complaint within two weeks of receipt and inform the Individual of the response procedure and timelines.

Step 2

- Investigate the circumstances of the Processing subject to the request or complaint and collect information relevant for a response.

Step 3

- Provide the Individual with information on any action taken further to their request or complaint without undue delay and, in any event, no later than one month of receipt of the request or complaint.
- If in the course of the investigation it is anticipated that the one month response deadline cannot be met taking into account the complexity and number of the requests or complaints and, where a Privacy Champion has been designated, in cooperation with the OE DPP/DPO, inform the Individual of any extension within one month of receipt of the request, together with the reasons for the delay, and the expected timeline for the request or complaint to be handled (such period to be no longer than two months, except in extraordinary circumstances). Where appropriate, the OE Privacy Champion or DPP/DPO may liaise with the GCPO to handle a complex request or complaint.

Step 4

- If the investigation reveals that the request or complaint is justified, cooperate with the OE Data Controller board of management and, where a Privacy Champion has been designated, cooperate with the relevant DPP/DPO, as well as with the GCPO, as appropriate, to implement relevant measures to address the request or resolve the complaint, inform the Individual (i) of the findings, (ii) the corresponding remediation measures, (iii) the right to escalate the request or complaint to the GCPO if they are dissatisfied with the result or the handling of their request or complaint, and (iv) the right to lodge a claim before the Court and a complaint before the Supervisory Authority.
- If the investigation reveals that the request or complaint is not justified, inform the Individual without undue delay, and in any event, no later than one month, of (i) the findings together with reasons, (ii) the right to escalate the request or complaint to the GCPO if they wish to challenge the response where the Individual's request or complaint is rejected, and (iii) the Individual's right to lodge a complaint with a competent EEA data protection authority, and to seek judicial remedies.

Where the Privacy Champion has been tasked by the DPP/DPO with handling requests and complaints, the Privacy Champion must keep the DPP/DPO apprised of all steps taken and any information learned.

III. Contact and form of response to an Individual

OE Data Controllers must provide Individuals with the contact details of the OE DPO/DPP in privacy notices to facilitate Individuals' exercise of such rights or complaints.

Where the Individual makes the request by electronic means, the OE Data Controller must provide any information by electronic means in a commonly used electronic form, where possible, unless otherwise requested by the Individual. If the information provided to the Individual includes Personal Data or confidential information, the OE Data Controller must adduce appropriate safeguards when providing them to the Individual, so as to ensure their safe transmission (*e.g.*, via encryption).

IV. Costs

Any communication and any action taken by the OE Data Controller in response to an Individual's exercise of their rights or a complaint must be provided free of charge, save that a reasonable fee may be charged if:

- Requests or complaints are manifestly unfounded or excessive, in particular because of their repetitive character, in which case the OE Data Controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the requests or complaints; or
- Further copies of their Personal Data are requested.

V. Refusal to act on an Individual's request or complaint

OE Data Controllers may refuse to act on any requests or complaints where:

- They are manifestly unfounded or excessive, in particular because of their repetitive character, and the OE Data Controller can demonstrate the manifestly unfounded or excessive character of the requests or complaints;
- Processing requires identification, and the OE Data Controller can demonstrate that it is not in a position to identify an Individual; or

- The right of the Individual is expressly restricted by applicable EEA laws and regulations.

In the event of requests to erase Personal Data, OE Data Controllers may also refuse to act if the Processing is necessary:

- To exercise the right of freedom of expression and information;
- To comply with EEA laws and regulations to which the OE Data Controller is subject which require Processing, or for the performance of a task carried out in the public interest or in the exercise of an official authority vested in the OE Data Controller; or
- To establish, exercise or defend legal claims.

VI. Notification to recipients

Where the request relates to the rights to rectify or erase Personal Data, or to restrict Processing, OE Data Controllers must:

- Communicate any rectification or erasure of Personal Data or restriction of Processing to each recipient to whom the Personal Data have been disclosed, unless this proves impossible or involves disproportionate effort; and
- Upon an Individual's request, inform the Individual of those recipients.

Annex D: APS Requirements Overview

		Global Minimum Requirements	EEA Processing Requirements
A.			
I.	Rationale	1	2
II.	Authorization and Updates	1	2
B.			
I.	Due Care	1	2
II.	Data Quality	1	2
1.1.	*Global Minimum Requirements*	1	2
1.2.	*Additional Requirements for EEA Processing*		2
2.	Data Minimisation and Accuracy	1	2
3.	Storage Limitation	1	2
III.	Global Transparency & Openness		
1.	Global Minimum Requirements	1	2
2.	Additional Requirements for EEA Processing		
2.1.	*Information collected from the Individual*		2
2.2.	*Information not collected from the Individual*		2
IV.	Lawfulness of Processing		
1.	Global Minimum Requirements	1	2
2.	Conditions of consent for EEA Processing		2
3.	Lawfulness of Sensitive Personal Data Processing for EEA Processing		2
4.	Lawfulness of Processing for criminal convictions and offences for EEA Processing		2
V.	Relationship with Data Processors		
1.	Global Minimum Requirements	1	2
2.	Additional Requirements for EEA Processing		2
VI.	Transfers & Onward Transfers		
1.	Global Minimum Requirements	1	2
2.	Additional Requirements for EEA Processing		2
VII.	Security & Confidentiality		
1.	Global Minimum Requirements	1	2
2.	Additional Requirements for EEA Processing		2
VIII.	Personal Data Breaches or Incidents		
1.	Global Minimum Requirements	1	2

2.	Additional Requirements for EEA Processing		2
2.1.	*Notification to the competent EEA data protection authority*		2
2.2.	*Communication to Individuals*		2
2.3.	*Notification to the Data Controller*		2
IX.	Privacy by Design and Default		
1.	Privacy by Design		
1.1.	*Global Minimum Requirements*	1	2
1.2.	*Additional Requirements for EEA Processing*		2
2.	Privacy by Default for EEA Processing		2
X.	Cooperation with EEA data protection authorities for EEA Processing		2

C.	**Data Privacy and Protection Compliance Activities and Processes**		
I.	Privacy Impact & Ethics Assessments and Records of Processing Activities	1	2
II.	Training		
1.	Global Minimum Requirements	1	2
III.	Internal Requests and Complaints Mechanism		
1.	Global Minimum Requirements		
2.	Additional Requirements for EEA Processing	1	2
IV.	Monitoring and Assurance		2
1.	Global Minimum Requirements		

D.	**Obligations towards Individuals**		
I.	Responding to Individuals' requests to access, rectify, or erase		
1.	Global Minimum Requirements		
2.	Additional Requirements for EEA Processing	1	2
2.1.	*Access request*		2
2.2.	*Rectification request*		2
2.3.	*Erasure request*		2
II.	Responding to Individuals' requests to object to EEA Processing		2
III.	Responding to Individuals' requests to restrict EEA Processing		2
IV.	Responding to Individuals' requests for portability for EEA Processing		2
V.	Responding to Individuals' requests to object to automated decisions for EEA Processing		2

E.	Roles and Responsibilities		
I.	Allianz Group Level		
1.	The Allianz SE Board of Management	1	2
2.	Group Privacy	1	2
3.	Group Chief Privacy Officer	1	2
II.	Allianz Regional Level & Global Lines	1	2
III.	Allianz OE Level		
1.	OE Board of Management		
1.1.	*Global Responsibilities*	1	2
1.2.	*Additional Responsibilities for EEA Processing*		2
2.	OE Data Privacy Professional/Data Protection Officer		
2.1.	*Global Responsibilities*	1	2
2.2.	*Additional Responsibilities for EEA Processing*		2
3.	OE Privacy Champions		
3.1.	*Global Responsibilities*	1	2
3.2.	*Additional Responsibilities for EEA Processing*		2
4.	OE Information Owner	1	2
IV.	Allianz Group and OE Steering	1	2
1.	Allianz Data Privacy and Protection community	1	2
2.	Allianz Privacy Advisory Group	1	2

F.	References	1	2
Annex A	Glossary	1	2
Annex B	Minimum Requirements for Data Controller - Data Processor Contractual Relationships for EEA Processing		2
Annex C	Handling of Individuals' Requests and Complaints relating to EEA Data		2

Document Information

Document:	Allianz Privacy Standard (APS)
Author(s):	Philipp Räther, Kully Thandi
Contact Person(s):	Group Privacy
Area of Application:	Allianz Group

Amendments and Updates

Version	Date	Reason for and Extent of Changes	Author(s)
2.0	April 10, 2018	Adoption of BCRs by the Allianz Group. This document supersedes and replaces the Allianz Standard for Data Protection and Privacy dated October 1, 2013.	Philipp Räther, Kully Thandi
2.1	[●]	Modification of the Allianz Privacy Standard to align it with the EU General Data Protection Regulation and the Article 29 Working Party's referential on BCRs (WP256) rev. 01 adopted February 6, 2018.	Philipp Räther, Kully Thandi, Jason Glass
3.0	November 30, 2020	Annual review incorporating minor changes, including the incorporation of the Functional Rule for Governance, Monitoring and Assurance into the Framework.	Philipp Räther, Jason Glass, Kathleen Ugalde
4.0	November 30, 2021	Annual review incorporating changes from the Bavarian Data Protection Authority concerning the implementation of requirements in Article 29 Working Party's referential on BCRs (WP256).	Jason Glass
5.0	November 2, 2022	Edits to divide the Allianz Privacy Standard from the BCRs, to incorporate changes from the Bavarian Data Protection Authority concerning the implementation of requirements in Article 29 Working Party's referential on BCRs (WP256) that must be reflected in both the Framework and BCRs, and to reflect GP move from business division H6 to H4. Small adjustments to further clarify Group Privacy Interfaces with other Control Functions.	Philipp Räther, Jason Glass, Kathleen Ugalde