Version 1.0

Effective:
01.05.2021

Allianz Privacy Standard Addendum

Classification: Internal

DRAFT

Authorization:

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

Version	Valid from	Authorized by (alternatively)	
		Group Center Head	Allianz SE Board Member
1.0	01-05-2021	Dr. Philipp Räther – Group Chief Privacy Officer	Renate Wagner

Table of Contents

Chapter	Content	Page
Introduction		**3**
A. Group Privacy		**3**
I.	Group Chief Privacy Officer	3
II.	Group Privacy interfaces	3
B. Regions		**5**
I.	Regional DPO	5
C. OE Privacy Governance		**5**
I.	OE Data Protection Officer (DPO) and Data Privacy Professional (DPP)	5
D. Privacy Monitoring and Assurance Framework		**6**
I.	Privacy Controls	6
II.	Independent reviews	6
III.	Quarterly reporting	6

Introduction

This document serves as Addendum to the Allianz Privacy Standard (APS) and applies to Allianz OEs accordingly. The APS applies to all 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.

A. Group Privacy

I. Group Chief Privacy Officer

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 define a Group-related target for the Regional DPOs and the OE DPOs/DPPs and shall be involved in the respective assessment process.

II. Group Privacy interfaces

Group Privacy has interfaces and close cooperation with other Group functions. The GCPO, encourages, considering OEs' specific interfacing needs, an equivalent level of close contact by OE Privacy functions with other functions corresponding to the below list.

1. Relationship with the Group Risk management function

Privacy risk is classified as an operational risk within the Group's overall risk categorization. Group Risk is defining the overarching principles, processes and responsibilities for the management of operational risk via the IRCS. Other risk-related procedures to assess Privacy risks are aligned between GP and Group Risk. GP is defining controls for Privacy.

2. Relationship with the Group Compliance function

GP and Group Compliance cooperate with regard to:

i. self-assessments of the controls implementation status by Regions/OEs (e.g. the annual Program Maturity assessment);
ii. monitoring activities for controls effectiveness testing (e.g. reviews).

In case of a Privacy complaint or a Personal Data Incident reported through Compliance channels, the Compliance function must inform the Privacy function in order to ensure timely handling of each case and vice versa.

3. Relationship with the Group Information Security (IS) function

The Group IS function is defining the Information-Security-related requirements for all processes and functions with regard to storing information that has a value to Allianz from a business perspective (cf. -> AFRIS definition Information Security). The information security requirements focus on the protection of confidentiality, integrity and availability of such information.

The Privacy and Information Security functions cooperate to protect the confidentiality, availability and integrity of Personal Data and to protect Personal Data against improper collection and processing.

The following responsibilities are derived:

i. Requirements towards identification, protection and treatment of Personal Data are defined by GP;
ii. Requirements towards proper encryption and other means to protect information classified as confidential are defined by the Group IS function (cf. AFRIS chapter E. & Annex B.);
iii. Requirements for the information classification (cf. AFRIS chapter D. and Annex B) are defined by the Group IS function and aligned with GP in regards to Personal Data;
iv. The Information Security Incident Handling process ensures that the Privacy function is involved by the IS function whenever Personal Data is or may be affected. The Personal Data Incident Management process ensures that the IS function is involved by the Privacy function whenever additionally to Personal Data also general information relevant for the business of Allianz is or may be affected;
v. Group IS and GP align on performing joint monitoring activities, event-related and for control effectiveness (e.g. peer reviews). Results from such monitoring activities that have a relevance for the other party will be shared between the two functions; and
vi. Group IS and GP align on a consolidated and unified management reporting for significant cases that impact both IS and Privacy.

4. Relationship with the Group Operations and Performance (GOP) function

GP is responsible to advise and monitor compliance with data protection laws and the Allianz privacy framework. GOP commits to promote and facilitate privacy by design for areas under GOP responsibility (that may include designing processes, common solutions and managing operations). Business owners retain responsibility to comply with the Allianz privacy framework.

GP and GOP, when necessary, liaise on matters affecting privacy compliance at Allianz, such as projects or initiatives with privacy implications driven by GOP and opportunities to collaborate on future regulatory change projects.

GP and GOP (P&R) cooperate to perform monitoring activities such as self-assessments and joint reviews and support consolidated and unified management reporting.

GP and GOP (Procurement): the Privacy function aligns with Procurement function on the sound implementation of Privacy relevant aspects in the Procurement framework such as data processing agreements, pre-contractual supplier due diligence activities and ongoing periodic supplier audit activities.

5. Relationship with the Group Legal function

The Group Privacy and Legal functions cooperate to ensure with regard to the interpretation of and adherence to the relevant Privacy regulations, statutes and other sources of law. Group Legal is responsible for the advice on contractual relationships and data protection agreements (Data Processing Agreements, EU Data Transfer Model Clauses, etc.). For data protection issues that arise outside of a specific contract context, e.g. websites privacy notices, Privacy Impact Assessments, BCRs, etc., GP remains responsible. Group Legal owns the Allianz Standard for Information and Document Management (ASIDM). In this regard GP decides on the maximum retention period for documents that do not need to be kept for legal or business reasons (non-relevant documents).

6. Relationship with the Group Internal Audit function

The Group Privacy function and Internal Audit functions (3rd line of defense) are separated with no reporting of one function into the other. However, this separation does not exclude the functions from jointly exercising specific tasks in the course of investigations. Group Audit must keep GP informed of all practice audit findings relating to Privacy.

Privacy is included in the audit program and methodology of the Internal Audit function, including a periodic assessment of the adequacy and effectiveness of the Group Privacy function. Based on the annual audit plan and scope, Group Privacy may rely on audit procedures performed by the Internal Audit function. This should be aligned and documented.

B. Regions

I. Regional DPO

1. Appropriate Resources

In determining the appropriate allocation of resources for the Regional DPO, the activities to be performed, the related capabilities needed by the Privacy function, the nature of the business, the complexity of its operations and the regulatory environment must be considered. In circumstances where an individual performs roles in addition to that of Regional DPO that could lead to conflict of interest, the proportion of time that the individual dedicates to executing the responsibilities of the Regional DPO must be documented and the Regional DPO may obtain advice from the GCPO on the matter.

2. Regional DPO Responsibilities

The Regional DPO must:

i. Oversee OEs' appropriate implementation of the Privacy framework and monitor, through Regional monitoring activities (e.g. annual program maturity assessment, 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 (e.g. reviews), in particular, the existence of local Privacy issues or audit findings, and coordinate timely remediation;
iii. Advise DPOs/DPPs within the Region on their obligations under the framework, including facilitating training on Privacy;
iv. Promptly inform GP of major regulatory investigations/actions and cooperate with the local DPOs/DPP to handle these;
v. Support, where applicable, local DPOs/DPPs cooperation with competent data protection authorities on privacy-related issues;
vi. Conduct at least quarterly calls with local DPOs/DPPs under their responsibility; and
vii. Participate in the Allianz Privacy Advisory Group ("APAG") upon request of the GCPO.

C. OE Privacy Governance

I. OE Data Protection Officer (DPO) and Data Privacy Professional (DPP)

1. Appropriate Resources

In determining the appropriate resources, the activities to be performed and related capabilities needed by the Privacy function, the nature of the business, the complexity of its operations and the regulatory environment must be considered. 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 and the OE may obtain advice from the GCPO or the assigned Regional DPO on the matter. For 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.

D. Privacy Monitoring and Assurance Framework

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

I. Privacy Controls

i. GP defines controls for Privacy. The controls are part of the IRCS and aligned with Group Risk. The IRCS controls for Privacy are mandatory for all OEs;
ii. OE DPOs/DPPs conduct self-assessments based on the corresponding control system (e.g. the annual Risk & Maturity assessment);
iii. GP and Regional DPOs conduct independent reviews to assess OEs' Privacy compliance status;
iv. OE DPOs/DPPs must perform monitoring activities (e.g. spot-checks, reviews) of Legal Entities / departments in scope for the OE.

II. Independent reviews

At least every 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. This review is conducted by GP and/or Regional DPOs.

GP adopts a risk-based methodology aimed at finding the most effective and efficient approach to select OEs for reviews.

The privacy issues identified during the independent reviews are monitored via a dedicated tool (e.g. Compliance Issue Management Tool) until remediation. 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.

III. Quarterly reporting

GP maintains a reporting program to obtain the information it deems 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 quality 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;
ii. Assign a point of contact (typically the DPO or DPP) to manage its reporting requirements.