СТАНДАРТ НА АЛИАНЦ ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

Класификация: За вътрешно ползване

Оторизации:

Съдържанието на този документ е ревизирано и одобрено, както следва:

Версия	Валидна от	Оторизирана от	Уведомление до Борда на Управление на Allianz SE
3.0	01.12.2020	Ренате Вагнер, 26.11.2020	03.12.2020
3.0	27.04.2021	Приет от УС на ЗАД Алианц България Живот	
3.0	27.04.2021	Приет от УС на ЗАД Алианц България	
3.0	29.04.2021	Приет от УС на ЗАД Енергия	
3.0	28.04.2021	Приет от УС на ПОД Алианц България	
3.0	24.02.2021	Приет от УС на Алианц Банк България	
3.0	17.05.2021	Приет от УС на Алианц Лизинг България	

I. Алианц е твърдо ангажирана с провеждането на бизнес в пълно съответствие и в съответствие с приложимите закони и разпоредби за защита на личните данни и защитата на данните. По този начин Алианц се стреми да защитава личните данни на физически лица, да защитава Алианц Груп и да насърчава доверието в Алианц като надежден доставчик на финансови продукти и услуги

II. Стандартът за поверителност на Allianz съдържа глобалните минимални изисквания, приложими в рамките на Allianz Group за обработка на лични данни, както и допълнителни условия за обработка на територията на Европейското Икономическо пространство/ ЕИП/ и за трансфер съгласно задължителните корпоративни правила /Binding Corporate Rules (BCRs). Като такъв, Стандартът за поверителност на Allianz представлява, inter alia, законово признатия механизъм на Allianz за узаконяване и улесняване на трансгранични трансфери на лични данни, произхождащи от или обработени в ЕИП в рамките на Allianz Group („Задължителни корпоративни правила /Binding Corporate Rules (BCRs; и

▪ Функционални правила, които допълнително определят изискванията за поверителност и защита на данните. Те се отнасят до управление на поверителността, мониторинг и осигуряване, оценки на въздействието и етиката върху поверителността и записи на обработка, обработка на заявки и жалби за достъп на субекти и управление на инциденти с лични данни!

III. Стандартът за поверителност на Allianz се прилага за Allianz Group. Той не обхваща информационната сигурност, запазването и изтриването на записи, управлението на инциденти, свързани с неприкосновеността на личните данни и защитата, и общата защита на бизнес тайните, които са предмет на изискванията на други стандарти на Allianz

IV. Управителният съвет на Allianz SE одобрява стандарта за поверителност на Allianz на 28 май 2018 г. Всички служители трябва да бъдат законово обвързани от неговите изисквания. Стандартът за поверителност на Allianz е правно обвързващ за юридическите лица на Allianz Group, които сключват вътрешнофирмено споразумение за прилагане на задължителните корпоративни правила на Allianz

V. ОЕ могат да разработят еквивалентни правила и процедури, за да се приведат в съответствие с изискванията на стандарта за поверителност на Allianz към съответната им бизнес структура или модел. Всички съществени отклонения от стандарта за поверителност на Allianz трябва да бъдат

предварително приведени в съответствие с поверителността на групата и да бъдат документирани правилно.

VI. Стандартът за защита на личните данни на Allianz е отговорност на подразделението на члена на Управителния съвет на Allianz SE, отговарящ за бизнес подразделението H6, с отговорност за поверителността на данните и функцията за спазване на защитата.

Съдържание

A. Въведение

I. Обосновка

1. Allianz се ангажира да защитава поверителността и правата за защита на данните на своите служители, клиенти, бизнес партньори и трети страни („Физически лица"). Този стандарт за защита на личните данни на Allianz („APS") е създаден, за да улесни спазването на приложимите закони и разпоредби за поверителност и защита на данните, които регулират Обработката и трансфера на лични данни. По-специално, APS предоставя рамка за обработване на лични данни, предмет на законите и разпоредбите на ЕИП в рамките на Allianz Group, и подходящи предпазни мерки за данните от ЕИП, прехвърлени към ОЕО извън ЕИП, както е описано в приложение Б. Като такова APS представлява, наред с другото, законово признатият механизъм на Allianz за легитимиране и улесняване на трансфери на лични данни, произхождащи от или обработвани в ЕИП в рамките на Allianz Group („Задължителни корпоративни правила" или „BCRs").

2. APS определя глобални минимални изисквания за поверителност и защита на данните за Обработка на лични данни от всички дружества на Алианц(„Минимални изисквания на глобално ниво", т. 1 по-долу). В допълнение, APS определя минимални изисквания за обработката на лични данни, предмет на законите и разпоредбите на ЕИП („Изисквания за обработка в ЕИП", т. 2 по-долу) и трансграничните трансфери на лични данни, предмет на законите и разпоредбите на ЕИП в рамките на Allianz Груп („Изисквания за трансфер, съгласно BCRs", т. 3 по-долу). Където е приложимо, в допълнение към минималните изисквания на глобално ниво се прилагат изискванията за обработка на територията наЕИП и изискванията за трансфери, съгласно BCRs. Следните точки показват, както следва в APS

- Приложими за обработка на лични данни като цяло („Минимални изисквания на глобално ниво“)
- Приложими при обработка на лични данни в съответствие със законите и разпоредбите на ЕИП („Изисквания за обработка в ЕИП“)
- Приложими за данни от ЕИП, прехвърлени в рамките на Allianz Group („Изисквания за трансфер, съгласно BCRs“)

Преглед на всички изисквания е предоставен в Приложение Е (Преглед на изискванията за APS

3. APS замества и заменя Стандарта за защита на личните данни /Allianz Privacy Standard 2.0 от 10 април 2018 г. APS се допълва от функционални правила/ Functional Rules/, посочени в глава F. APS и съответните му функционални правила заедно формират Рамката за поверителност и защита на данните на Allianz („Рамка“ ") / the Allianz Data Privacy and Protection Framework ("Framework").

4. APS се прилага за Allianz Group. Всички ОЕ и служителите трябва да са правно обвързани с неговите изисквания. APS е правно обвързваща за юридическите лица на Allianz Group, които сключват вътрешнофирмено споразумение за прилагане на BCR на Allianz („ICA“).

5. ОЕ трябва да прилагат Рамката/ Framework/ ефективно, в съответствие със законовите изисквания в съответните им юрисдикции и да съобщават рамката на всички съответни адресати

6. По подразбиране изискванията на APS се отнасят както за ОЕ, действащи като администратори на данни /Data Controllers/, така и за ОЕ обработващи /Data Processors/, действащи като обработващи данни от името на ОЕ администратори, освен ако не е посочено друго. Освен там, където Изискванията за обработка на ЕИП и BCR прехвърляния се отнасят само за ОЕ администратори на данни, ОЕ обработващите данни трябва да се придържат към стандартите, наложени на тези ОЕ администратори на данни, и да улеснят способността на ОЕ администраторите на данни да се съобразяват с тези стандарти

7. APS не обхваща информационната сигурност, съхраняването и изтриването на записи, управлението на инциденти, свързани с

неприкосновеността на личните данни и защитата, както и общата защита на бизнес тайните, които са предмет на изискванията на други стандарти на Allianz.

8. Ако някоя част от APS е по-малко строга от местните закони или разпоредби, такива местни закони или разпоредби ще имат предимство. В случай на неяснота между глобалните минимални изисквания, изискванията за обработка на ЕИП и изискванията за прехвърляне на BCR, изискванията за обработка на ЕИП и изискванията за прехвърляне на BCR ще имат предимство. В случай на някаква несигурност, съответният професионалист за защита на личните данни на ОЕ („DPP“) / Длъжностното лице по защита на данните („DPO“) (чиито роли и отговорности са определени в глава Е, раздел II.2 по-долу) трябва да се консултира с функцията по Защита на данните на Групата („Group Privacy“, "GP"), за да разреши конфликта.

9. Главният служител на Групата за поверителност (The Group Chief Privacy Officer „GCPO“) може по свое усмотрение да се откаже изцяло или частично от всяко Минимално Глобално Изискване за който и да е администратор на данни или обработващ данни извън ЕИП, за които изискванията относно обработка в ЕИП и изискванията за BCRs Трансферите са неприложими. GCPO трябва да документира писмено всяко изключение от глобалните минимални изисквания и мотивите в подкрепа на това решение.

II. Одобрение и актуализации

На члена на управителния съвет на Allianz SE, отговарящ за бизнес отдел H6, е възложена обща отговорност за Group Privacy (GP). GP е собственик на APS и му е възложена отговорността да поддържа и актуализира APS. APS трябва да се преразглежда поне веднъж годишно. APS трябва да бъде одобрен от члена на Управителния съвет на Allianz SE, отговарящ за бизнес подразделението H6, и надлежно отбелязан от Управителния съвет на Allianz SE.

Рамката /The Framework/ е достъпна в Корпоративния правилник /Corporate Rule Book /на Allianz Connect. Публична версия на APS, включително изискванията, приложими за физически лица, процедурите за искания и жалби, описани в приложение D, както и актуален списък на юридическите лица на Allianz Group, които са влезли в Inta-Company Agreement (ICA), е на разположение на www.allianz.com/en/info/privacystatement/.

APS (версия 3.0) ще се прилага от датата на уведомяване на Управителния съвет на Allianz SE. APS (версия 3.0) замества и заменя Стандарта за защита на личните данни Allianz 2.1 от 10 април 2018 г., който, доколкото е приложимо за ОЕ, прилагани до 24 май 2018 г.

B. Принципи за спазване на изискванията за поверителност и защитата на данните

I. Дължима грижа

1 2 3 Администраторите на данни за ОЕ/ OE Data Controllers/ трябва да обработват личните данни с дължимата грижа, законно, честно и по прозрачен начин.

II. Качество на данните

1. Ограничаване на целта

2 3 2 #### 1.1. Минимални изисквания на глобално ниво

Администраторите на данни за ОЕ трябва да обработват лични данни за конкретни, изрични и законни бизнес цели и в съответствие със следното:

- Приложими закони и разпоредби, включително професионална поверителност;
- Изисквания за информационна сигурност, съдържащи се в Рамката за информационна сигурност на Allianz Group (GISF); и
- Изисквания за задържане и изтриване на данни, съдържащи се в Стандарта за управление на информация и документи Allianz (ASIDM).

Администраторите на данни за ОЕ / OE Data Controllers трябва да обработват лични данни само до степента, която е от съществено значение за изпълнение на посочените бизнес цели.

Администраторите на данни за ОЕ / OE Data Controllers могат да извършват последващи промени в посочените бизнес цели, при условие че тези промени са посочени, изрични и легитимни

3 2 #### 1.2. Допълнителни изисквания за обработка в ЕИП и трансфери съгласно BCRs

Администраторите на данни за ОЕ могат да извършват последващи промени в посочените бизнес цели, при условие че това не е несъвместимо с първоначалните цели

2. Минимизиране и точност на данните

Администраторите на данни за ОЕ трябва да гарантират, че:

- Личните данни се актуализират и всички неточности се изтриват и коригират незабавно, като се имат предвид целите, за които се обработват;
- Всички актуализации на Личните данни се отразяват във всички системи и бази данни, независимо дали са вътрешни или външни; и
- Личните данни са адекватни и ограничени до необходимото за целите, за които личните данни трябва да бъдат обработвани.

3. Ограничение на съхранението

Администраторите на данни за ОЕ трябва да съхраняват лични данни толкова дълго, колкото е необходимо за изпълнение на определени бизнес цели или както се изисква от приложимите закони и разпоредби и в съответствие с изискванията за съхранение и изтриване на данни на Allianz, съдържащи се в Стандарта за управление на информация и документи (ASIDM) на Allianz.

Администраторите на данни за ОЕ трябва да унищожават и архивират по подходящ начин личните данни в съответствие с приложимите закони и разпоредби и изискванията за запазване и изтриване на данни на Allianz, съдържащи се в Стандарта за управление на информация и документи (ASIDM) на Allianz.

Като алтернатива на унищожаването, ОЕ администраторите на данни могат да анонимизират личните данни

III. Прозрачност и откритост

1. Минимални изисквания на глобално ниво

Администраторите на данни за ОЕ трябва да информират физическите лица, в съответствие с приложимите закони и разпоредби, по време на събирането и при ясни и достъпни условия, за целите, за които се събират техните лични данни, как те трябва да бъдат обработвани и, ако е приложимо, на кого ще бъдат прехвърлени

Администраторите на данни за ОЕ трябва да гарантират, че личните данни се събират предимно директно от съответното лице и се събират само от трети страни или други източници, при условие че това е разумно и разрешено от приложимите закони и разпоредби.

2. Допълнителни изисквания за обработка в ЕИП и за трансфери съгласно BCRs

2.1. Информация, събрана от физическото лице

Администраторите на данни за ОЕ трябва да предоставят на физическите лица информацията, посочена по-долу, писмено или по друг начин, включително, когато е уместно, в електронна форма. Той трябва да бъде предоставен в кратка, прозрачна, разбираема и лесно достъпна форма на достъпен и ясен език:

- Името и данните за контакт на ОЕ Администратор на данни или негов представител
- Данните за контакт на ОЕ DPP / DPO, където е приложимо;
- Целите на Обработването, за които са предназначени Личните данни, и правното основание за Обработката;
- Законният интерес, преследван от Администратора на данни или от трета страна, когато такъв интерес предоставя правното основание за Обработката;
- Получателите или категориите получатели на Личните данни;
- В случай на прехвърляне в страни извън ЕИП, предпазните мерки, приложени за защита на прехвърлените Лични данни, и средствата, чрез които физическо лице може да получи копие от тях или когато те са били предоставени;
- Периодът, за който ще се съхраняват Личните данни или, ако не е възможно, критериите, използвани за определяне на този период;
    - Наличието на права на физическите лица относно:
    - Достъп, коригиране и изтриване на лични данни;
    - Ограничаване на обработката;
    - Преносимост на данните;
    - Възражение за обработка. Това право трябва да бъде изрично обърнато на вниманието на физическото лице, ясно и отделно от всяка друга информация, когато Обработката се основава на законния интерес на Администратора на данни или когато Личните данни се обработват за целите на директния маркетинг;
    - Оттегляне на съгласието си по всяко време, когато съгласието предоставя правно основание за обработката на лични данни или чувствителни лични данни. Такова оттегляне не трябва да засяга законността на обработката, извършена преди искането на физическото лице за оттегляне на неговото / нейното съгласие; и
    - да подаде жалба пред компетентен орган на ЕИП за защита на данните;
- Дали предоставянето на лични данни е законово или договорно изискване, или изискване, необходимо за сключване на договор, както

и дали физическото лице е задължено да предостави личните данни, както и от възможните последици от това и
- Съществуването на автоматизирано вземане на решения, включително профилиране, и значима информация за съответната логика, както и значението и предвидените последици от тази обработка за индивида.

Администраторите на данни за ОЕ, които възнамеряват да обработват лични данни за цели, различни от първоначалната цел, трябва да информират засегнатите лица преди по-нататъшната обработка с информация за тази друга цел, както и всякаква съответна информация, изброена по-горе

2.2 Информация, която не е събрана от физическото лице

Когато лични данни не се получават от физически лица, администраторите на ОЕ данни трябва да им предоставят подробности за следното, в допълнение към информацията, изброена в глава B, раздел III.2.2.1. горе

- Засегнатите категории лични данни; и
- Източникът на личните данни и, ако е приложимо, дали от публично достъпни източници

Администраторите на данни за ОЕ трябва да предоставят такава информация на физическите лица

- В рамките на един месец от получаването на личните данни, като се вземат предвид конкретните обстоятелства, при които се обработват личните данни;
- Ако личните данни ще се използват за комуникация с физически лица, за които се отнасят личните данни, най-късно в момента на първата комуникация с тези физически лица; или
- Ако се предвижда разкриване пред друг получател, най-късно при първото разкриване на личните данни

Администраторите на данни за ОЕ, които възнамеряват да обработват лични данни за цели, различни от първоначалната цел, трябва да информират засегнатите лица преди по-нататъшната обработка с информация за тази друга цел, както и всякаква съответна информация, изброена по-горе. Администраторите на данни за ОЕ не е необходимо да предоставят такава информация на физически лица, ако:

- Те вече разполагат с такава информация
- Това ще се окаже невъзможно или ще включва прекомерни усилия
- Получаването или разкриването на лични данни се изисква изрично от приложимите закони и разпоредби на ЕИП; или

- Личните данни трябва да останат поверителни при спазване на задължение за професионална тайна, изисквано от приложимите закони и разпоредби на ЕИП

IV. Законосъобразност на обработването

1. Минимални изисквания на глобално ниво

Администраторите на данни за ОЕ трябва да обработват лични данни само ако има законово основание за това, както следва:

- Обработката е необходима за изпълнение на договор, по който физическото лице е страна, или за да се предприемат стъпки по искане на физическото лице преди сключване на договор;
- Обработката е необходима за спазване на законово задължение, по което администратора на данни е обект
- Обработката е необходима за защита на съществените интереси на физическото лице или на друго физическо лице
- Обработката е необходима за изпълнение на задача от обществен интерес или за упражняване на официална власт, поверена на Администратора на данни;
- Обработката е необходима за законните интереси на Администратора на данни или на трета страна, освен когато тези законни интереси са заменени от интересите или основните права и свободи на физическото лице, които изискват защита; или
- Със съгласието на физическото лице, където е приложимо при спазване на условията, посочени в глава B, раздел IV.2 по-долу.

2. Условия за съгласие при обработка в ЕИП и за трансфери съгласно BCRs

Когато личните данни се обработват въз основа на съгласието на физическо лице, администраторите на ОЕ данни трябва

- Да се уверят, че съгласието е дадено свободно, конкретно, информирано и недвусмислено посочва желанията на физическото лице (чрез изявление или ясна утвърдителна дейност) да се съгласи с обработването
- Да гарантира, че лицето има правода оттегли своето съгласие лесно (чрез изявление или ясна утвърдителна дейност), и е получило това право преди даване на съгласие за обработката.
- Да прилагат и поддържат процеси за записване на даването и оттеглянето на съгласие; и
- Да се уверят, че ако съгласието е дадено като част от писмена декларация, отнасяща се и до други въпроси, то ще бъде представено

по начин, който ясно се различава от другите въпроси, в разбираема форма, на достъпен и разбираем език.

3. Законосъобразност при обработка на чувствителни лични данни в ЕИП и при трансфери съгласно BCRs

Администраторите на данни за ОЕ трябва да внедрят и поддържат процеси, за да идентифицират къде се обработват чувствителни лични данни и да гарантират, че чувствителните лични данни се обработват само ако:

- Обработката е необходима:
  - Администраторът на данни или физическото лице да изпълнява или упражнява специфични права съгласно приложимото законодателство за трудова и социална сигурност и социална защита, доколкото това е разрешено от приложимите закони и разпоредби на ЕИП;
  - Защита на жизненоважните интереси на физическото лице или на друго физическо лице, когато физическото или юридическото лице не е в състояние да даде съгласие;
  - За установяване, упражняване или защита на правни искове или когато съдилищата действат в качеството си на съдебна власт;
  - За целите на превантивната или трудовата медицина, за оценка на работоспособността на служител, медицинска диагноза, осигуряване на здравни или социални грижи или лечение или управление на здравни или социални системи и услуги съгласно приложимите закони и разпоредби на ЕИП или по силата на договор със здравен специалист, предмет на задължението за професионална тайна или от друго лице, което също е обект на еквивалентно задължение за тайна;
  - За обществения интерес в областта на общественото здраве, като защита срещу сериозни трансгранични заплахи за здравето или осигуряване на високи стандарти за качество и безопасност на здравните грижи и на лекарствени продукти или медицински изделия, въз основа на приложимите закони на ЕИП и разпоредби, които предвиждат подходящи и специфични мерки за защита на правата и свободите на физическото лице, по-специално професионалната тайна;
  - По причини от съществен обществен интерес, съгласно приложимите закони и разпоредби на ЕИП, които трябва да са пропорционални на преследваната цел, да зачитат същността на правото на поверителност и защита на данните и да предвиждат подходящи и специфични мерки за защита на основните права на лицата и интереси; или
  - За целите на архивирането в обществен интерес, научни или исторически изследователски цели или статистически цели в

съответствие с приложимите закони и разпоредби на ЕИП, които трябва да бъдат пропорционални на преследваната цел, да зачитат същността на правото на поверителност и защита на данните и да предвиждат подходящи и специфични мерки за защита на основните права и интереси на лицето

- Обработката се отнася до чувствителни лични данни, които са явно публично оповестени от физическото лице; или
- Физическото лице е дало съгласието си за обработката за една или повече конкретни цели, освен когато това е забранено от приложимите закони и разпоредби на ЕИП.

4. Законосъобразност на обработването за наказателни присъди и престъпления за обработка в ЕИП и при трансфери съгласно BCRs

Администраторите на данни за ОЕ не могат да обработват лични данни, свързани с наказателни присъди и престъпления или свързани с мерки за сигурност, различни от под контрола на официален орган, или когато обработването е разрешено от приложимите закони и разпоредби на ЕИП, осигуряващи адекватни гаранции за правата и свободите на физически лица

V. Връзка с Обработващите данни / Data Processors

1. Минимални изисквания на глобално ниво

Личните данни могат да бъдат обработвани от обработващите данни само от името на администраторите на данни на ОЕ чрез писмено споразумение.

Администраторите на данни за ОЕ трябва:

- Да извършват комплексна проверка и преценка на риска за оценяване на обработващите данни, за да се провери дали тези обработващи данни могат да осигурят подходящи технически и организационни мерки в съответствие с GISF и да осигурят ниво на сигурност, подходящо за нивото на защита и поверителността на обработваните лични данни ; и
- Периодично да наблюдават обработващите данни, за да се провери текущото спазване на техните договорни задължения и задължения за съответствие.

2. Допълнителни изисквания за обработка в ЕИП и трансфери съгласно BCRs

Администраторите на данни за ОЕ трябва:

Да се уверят, че обработващите данни могат да предоставят достатъчни гаранции по отношение на техническите и организационни мерки, регулиращи предвидената обработка, така че обработката да отговаря на изискванията за сигурност и поверителност, посочени в глава B, раздел VII.2 .; и

Когато бъдещият обработващ данни не е член на Allianz Group, сключи писмено споразумение с потенциалния обработващ данни, съдържащо приложимите минимални изисквания, посочени в приложение B (Минимални изисквания за администратора на данни - договорни отношения за обработка на данни за ЕИП и трансфери съгласно BCRs); или, когато бъдещият обработващ данни е обработващ данни на ОЕ, се придържат към вътрешнофирмените условия за обработка на данни, както е приложено в списък 1 към Приложение C.

VI. Трансфери и последващи трансфери

1. Минимални изисквания на глобално ниво

Администраторите на данни за ОЕ и обработващите данни за ОЕ трябва да разкриват, споделят или прехвърлят лични данни на други ОЕ в съответствие с APS.

Администраторите на данни за ОЕ и обработващите данни за ОЕ трябва да разкриват, споделят или прехвърлят само Лични данни на администратори на данни или обработващи данни, които не са членове на Allianz Group в съответствие с APS и въз основа на писмени договори, освен ако такова споделяне или прехвърляне не е изрично разрешено от приложимите закони и разпоредби. Когато такова разкриване, споделяне или прехвърляне се извършва за цели, различни от посочената бизнес цел, то трябва да се извършва само ако е разрешено от приложимите закони или разпоредби или с изричното съгласие на физическото лице.

2. Допълнителни изисквания за обработка в ЕИП и трансфери на BCR

Администраторите на данни за ОЕ и обработващите данни за ОЕ могат да прехвърлят лични данни към ОЕ-страни извън ЕИП (действащи като администратори на данни или обработващи данни), които отговарят на изискванията за BCR трансфери и които са страна по ICA.

Прехвърляне на лични данни към ОЕ, които не са страни по ЕИП, които не са страна по ICA, или от ОЕ на ЕИП към Администратори на данни извън ЕИП или обработващи данни, които не са членове на Allianz Group, или по-нататъшни прехвърляния на лични данни от ОЕ извън ЕИП към Администраторите на данни или обработващите данни, които не са членове на Allianz Group, са разрешени въз основа на следното:

Решение за адекватност, издадено от Европейската комисия; или

- Администраторът на данни или обработващият данни, предоставящ подходящи предпазни мерки по отношение на прехвърлените Лични данни (например чрез стандартни клаузи за защита на данните, приети от Европейската комисия или орган за защита на данните в ЕИП) в съответствие с приложимите закони и разпоредби на ЕИП; или
- В специфичните и ограничени ситуации, разрешени от приложимите закони и разпоредби на ЕИП (напр. Изрично и информирано съгласие на физическото лице за прехвърлянето; прехвърляне, необходимо за изпълнението на договор между физическото лице и администратора на данни); или
- В краен случай, ако прехвърлянето е необходимо за целите на непреодолими законни интереси, преследвани от Администратора на данни, предоставен:

    - Прехвърлянето не се повтаря и се отнася само до ограничен брой лица;
    - Законните интереси на Администратора на данни не са заменени от Лични интереси или права и свободи;
    - Администраторът на данни е оценил и документирал всички обстоятелства около прехвърлянето и въз основа на това е предоставил подходящи предпазни мерки по отношение на поверителността и защитата на данните; и
    - Администраторът на данни информира компетентния орган за защита на данните в ЕИП и физическото лице за прехвърлянето и непреодолимите законни интереси

VII. Сигурност и поверителност

1. Минимални изисквания на глобално ниво

Администраторите на данни за ОЕ и обработващите данни за ОЕ трябва да обработват лични данни в съответствие с Рамката за информационна сигурност на Allianz Group (GISF).

2. Допълнителни изисквания за обработка в ЕИП и трансфери съгласно BCR

Администраторите на данни за ОЕ и обработващите данни за ОЕ трябва да приемат предпазни мерки срещу рисковете, свързани с обработката на лични данни, особено от загуба, случайно или незаконно унищожаване, изменение, неразрешено разкриване или достъп до лични данни, предадени, съхранени или обработени по друг начин

Като се вземат предвид състоянието на техниката, разходите за изпълнение, естеството, обхватът, контекстът и целите на обработката, както и тежестта и вероятността от рискове за правата и свободите на лицата, администраторите на данни за ОЕ и обработващите данни на ОЕ трябва да прилагат подходящи технически и организационни мерки за осигуряване на ниво на сигурност, подходящо за риска, като

- Анонимизиране на лични данни;
- Псевдонимизацията и криптирането на лични данни;
- Способността да се осигури постоянната поверителност, целостта, наличността и устойчивостта на системите и услугите за обработка;
- Възможност за своевременно възстановяване на наличността и достъпа до лични данни в случай на физически или технически инцидент;
- Процеси за редовно тестване, оценка и оценка на ефективността на техническите и организационни мерки за осигуряване на сигурността на обработката;
- Процедури, за да се гарантира, че всяко физическо лице, действащо под ръководството на Администратора на данни или Обработващия Данни, което има достъп до Лични данни, не обработва Лични данни, освен по указания от Администратора на данни, освен ако от него / тя се изисква да го направи от приложими закони и разпоредби на ЕИП; или
- Планове за непрекъснатост на бизнеса и възстановяване при бедствия.

VIII. Инциденти или нарушения на лични данни

1. Минимални изисквания на глобално ниво

Администраторите на данни за ОЕ и обработващите данни за ОЕ трябва да прилагат и поддържат ефективни процеси, за да осигурят своевременно уведомяване на ОЕ DPP / DPO в случай на инцидент или нарушение на личните данни.

Администраторите на данни за ОЕ и обработващите данни за ОЕ трябва да информират Group Privacy за всякакви комуникации до или от отговорния

надзорен орган, които задействат или е вероятно да задействат регулаторно разследване на поверителността на данните и практиките за защита на OE Data Controller или OE Data Processor в никакъв случай администраторът на данни на OE или обработващият данни на OE не може да приеме регулаторна санкция без предварителна консултация с GP.

Допълнителни изисквания са посочени във Функционалното правило за управление на инциденти с лични данни, Стандарт за защита и устойчивост на Allianz (AZ P&R стандарт), Функционално правило за защита и устойчивост на Allianz (AZ P&R Функционално правило) и Функционално правило за информационна сигурност на Allianz (AFRIS), както и в други политики и стандарти на Allianz, които могат да бъдат съобщени на OE от време на време.

2. Допълнителни изисквания за обработка в ЕИП и трансфери съгласно BCR

Администраторите на данни за OE и обработващите данни за OE трябва да внедрят и поддържат процеси за оценка на приложимите задължения за поверителност и уведомяване за защита на данните, включително уведомяване на компетентните органи за защита на данните в ЕИП, физически лица и администратори на данни.

2.1. Нотификация до компетентния орган за защита на данните в ЕИП

Администраторите на данни за OE трябва, без неоправдано забавяне и, когато е възможно, не по-късно от 72 часа, след като узнаят за нарушение на личните данни, което може да доведе до риск за правата и свободите на дадено лице, да документират и уведомят за нарушаването на личните данни до компетентния орган за защита на данните в ЕИП и уведомява без ненужно забавяне OE DPP / DPO и GP за следното:

- Естеството на нарушението на личните данни, включително, когато е възможно, категориите и приблизителния брой засегнати лица, категориите и приблизителния брой на съответните записи на лични данни;
- Името и данните за контакт на OE DPP / DPO или друга точка за контакт, от която може да се получи допълнителна информация;
- Вероятните последици от нарушаването на личните данни; и
- Мерките, предприети или предложени да бъдат предприети за преодоляване на нарушението на личните данни, включително, когато е подходящо, мерки за смекчаване на възможните неблагоприятни ефекти.

Ако такава информация не може да бъде предоставена едновременно, тя може да бъде предоставена на етапи без неоправдано допълнително забавяне.

2.2. Комуникация с лицата

Администраторите на данни за ОЕ трябва без неоправдано забавяне да информират засегнатото лице за нарушение на личните данни, ако има вероятност да доведе до висок риск за правата и свободите на лицето, описвайки на достъпен и ясен език:

- Естеството на нарушението на личните данни;
- Името и данните за контакт на ОЕ DPP / DPO или друга точка за контакт, от която може да се получи допълнителна информация;
- Вероятните последици от нарушаването на личните данни; и
- Мерките, предприети или предложени да бъдат предприети за преодоляване на нарушенията на личните данни, включително, когато е подходящо, мерки за смекчаване на възможните неблагоприятни ефекти.

Администраторите на данни за ОЕ не е необходимо да осигуряват такава комуникация, ако:

- Приложени са подходящи технически и организационни мерки за защита и тези мерки са приложени към личните данни, засегнати от нарушаването на личните данни, особено тези, които правят личните данни неразбираеми за всяко лице, което не е упълномощено да има достъп до тях (например криптиране);
- Предприемат се последващи мерки, за да се гарантира, че високият риск за правата и свободите на физическото лице е малко вероятно да се реализира; или
- Това би включвало непропорционални усилия, като в този случай трябва да се направи публично изявление или подобна мярка за информиране на засегнатите лица по еднакво ефективен начин.

2.3. Известие до администратора на данни

Обработващите данни на ОЕ трябва, без ненужно забавяне, но не по-късно от 24 часа, след като узнаят за нарушение на личните данни, да уведомят администратора на данни.

IX. Поверителност на етапа на проектиране и по подразбиране

I Поверителност на етапа на проектиране

1.1. Минимални изисквания на глобално ниво

Администраторите на данни за ОЕ трябва да гарантират, че поверителността и защитата на данните са методично вградени в съответните бизнес процеси и процедури и интегрирани в засегнатите ИТ системи и приложения.

1.2. Допълнителни изисквания за обработка в ЕИП и трансфери съгласно BCR

Администраторите на данни за ОЕ трябва да прилагат подходящи технически и организационни мерки (напр. Псевдонимизация), за да прилагат принципите за поверителност и защита на данните (например минимизиране на данните) в нови продукти, услуги и бизнес процеси и процедури, където е приложимо, по ефективен начин и да интегрират ефективно необходимите предпазни мерки при обработката на лични данни.

Администраторите на данни за ОЕ трябва да прилагат такива мерки както по време на определяне на средствата за обработка, така и по време на самата обработка.

Администраторите на данни за ОЕ трябва да вземат предвид състоянието на техниката, разходите за изпълнение и естеството, обхвата, контекста и целите на обработването, както и тежестта и вероятността от рискове за правата и свободите на лицата, породени от обработката

2. Поверителност по подразбиране за обработка в ЕИП и трансфери съгласно BCR

Администраторите на данни за ОЕ трябва да прилагат подходящи технически и организационни мерки, за да гарантират, че по подразбиране се обработват само Лични данни, необходими за всяка конкретна цел на обработката. Такова изискване се прилага за количеството събрани лични данни, степента на обработка и периода на съхранение и достъп. По-специално, по подразбиране личните данни не трябва да бъдат достъпни за неопределен брой физически лица без намесата на физическото лице (напр. Обратната връзка или коментарите, изпратени онлайн, не трябва да се публикуват по подразбиране).

X. Сътрудничество с органите за защита на данните в ЕИП за обработка на ЕИП и трансфери съгласно BCR

Администраторите на данни за ОЕ и обработващите данни за ОЕ трябва да си сътрудничат защитни органи от ЕИП при изпълнението на техните задачи и да се съобразяват със съветите на органите за защита на данните в ЕИП по всякакви въпроси, свързани с Изискванията за прехвърляне на BCR

C. Дейности и процеси за спазване на поверителността и защитата на данните

Следните дейности и процеси за съответствие са предназначени да улеснят спазването на принципите, изложени в глава Б и да подкрепят задълженията на ОЕ към лицата, посочени в глава D.

I. Оценки на въздействието върху поверителността и етиката и записи на обработката

3 3 2 Където е приложимо, OEs трябва да запишат своите дейности по обработка, както и да извършат оценка на въздействието върху поверителността („PIA“) или за обработка на дейности, използващи изкуствен интелект, Оценка на въздействието и етиката на поверителността. Както е описано по-нататък във Функционалното правило за оценка на въздействието върху неприкосновеността на личните данни и етиката при обработка на записи:

(i) Администраторите на лични данни трябва да анализират всички дейности по обработване, които представляват висок риск за поверителността на данните и защитата на приложимите законови, регулаторни и вътрешни изисквания на политиката;

(ii) Администраторите на данни трябва да определят действия за отстраняване на рисковете за поверителността, установени при изпълнението на горепосочените дейности; и

(iii) Администраторите на лични данни и обработващите лични данни трябва да създават и поддържат записи за всички свързани с обработването дейности, включващи лични данни

II. Обучение

3 1 1 **1.Минимални изисквания на глобално ниво**

Администраторите на данни за ОЕ и обработващите данни за ОЕ трябва да създават и провеждат периодични обучения за поверителност и защита на

данните за служители и друг персонал, за да осигурят адекватно ниво на знания и осведоменост.

2. Допълнителни изисквания за BCR трансфери

Администраторите на данни за ОЕ и обработващите данни на ОЕ трябва да предоставят на служителите и други лица от персонала, участващи постоянно или редовно в обработката или в разработването на инструменти, използвани за обработка на лични данни в ЕИП, подходящо обучение за поверителност и защита на данните, включително относно изискванията за обработка на ЕИП и изискванията за BCRs Трансфери.

Администраторите и обработващите лични данни трябва да се възползват от компютърно обучение, което се разработва и поддържа от Group Privacy. Разбирането на участниците ще бъде подложено на тест, като част от обучението. Администраторите на данни и обработващите данни трябва да проследяват степента на завършване на теста и изпълнението до степента, позволена от приложимите закони и разпоредби. Администраторите и обработващите данни трябва да гарантират, че служителите и останалия персонал запознати отговорностите си относно защита на неприкосновеността на личните данни към ЕАОС, например чрез използване на компонент за обновяване, разработен от Group Privacy. Честотата и съдържанието на опреснителните обучения са по усмотрение на главния директор по поверителността на групата (GCPO), но ще бъдат задължителни за всички OEs, освен тези, които не са изрично освободени от GCPO.

III.Вътрешен механизъм за обработване на оплаквания

1.Минимални изисквания на глобално ниво

Администраторите на данни за ОЕ трябва да прилагат и поддържат ефективни процеси за справяне със запитванията, жалбите и инцидентите, свързани с поверителността на данните и защитата.

2. Допълнителни изисквания за обработка в ЕИП и трансфери съгласно BCRs

При запивания от физически лица, свързани с техните права, посочени в глава Г, както и жалби, свързани с прехвърляния на BCR, администраторите на данни на ОЕ трябва да се придържат към процедурата, посочена в

приложение D (Обработка на молби и жалби на физически лица, свързани с данни от ЕИП).

III. Мониторинг и осигуряване

1.Минимални изисквания на глобално ниво

Администраторите на данни за ОЕ и обработващите данни за ОЕ, глобалните линии, региони и поверителността на групата трябва да извършват надзор, основан на риска (който може да включва мониторинг, тестване, прегледи, одити и други компоненти) на адекватния смисъл, изпълнение и ефективност на рамката и свързаните с тях процеси и контрол в рамките на 5-годишен цикъл, включително чрез проби, проучвания и прегледи.

Резултатите трябва да бъдат одобрени от Управителния съвет на ОЕ и да бъдат споделени - включително всяко съществено отклонение от Рамката, с GCPO (и където е приложимо за тяхната регионална / глобална линия DPP / DPO) своевременно.

Администраторите на данни за ОЕ и процесорите за обработка на данни трябва да предоставят изявления за отчетност във връзка с рамката, когато се изисква от GCPO.

Допълнителни подробности са описани във Функционалното правило за управление, наблюдение и осигуряване на поверителност.

3. Допълнителни изисквания за BCR трансфери

Администраторите на данни за ОЕ и обработващите данни на ОЕ трябва редовно да участват в одитите за защита на данните и защитата на данните (най-малко на всеки 5 години) или по конкретното искане на GCPO или партньор на ОЕ.

Такива одити трябва да се извършват от акредитирани професионалисти (вътрешни или външни) и да покриват Изискванията за прехвърляне (BCR), включително методи за осигуряване на ефективно проследяване и прилагане на действия за отстраняване.

Резултатите от одита трябва да бъдат съобщени на ОЕ DPP / DPO, управителния съвет на ОЕ, GCPO, на Управителния съвет на Allianz SE относно определянето на GCPO и, при поискване, на всеки орган за защита на данните в ЕИП.

Администраторите на данни за ОЕ и обработващите данни могат да бъдат одитирани от органите за защита на данните в ЕИП. ОЕ трябва незабавно да информират ОЕ DPP / DPO и GCPO (и, ако е приложимо, тяхната регионална

/ глобална линия DPP / DPO), ако някой орган за защита на данните в ЕИП поиска резултати от одит или възнамерява да извърши одит за поверителност и защита на данните.

D. Задължения към физически лица

I. Отговор на оплакванията на лица за достъп, коригиране или изтриване

1.Минимални изисквания на глобално ниво

Администраторите на данни за ОЕ трябва да предоставят на физическите лица възможността да преглеждат, коригират или изтриват своите лични данни, при поискване и в съответствие с приложимите закони и разпоредби, при условие че физическите лица първо удостоверяват своята самоличност до подходящо ниво на сигурност

Когато исканията са отказани, на лицата трябва да бъдат посочени причини за такъв отказ, заедно с правото да оспорят такова решение.

2. Допълнителни изисквания за обработка в ЕИП и трансфери на BCR

Администраторите на данни за ОЕ трябва да се придържат към процедурата, посочена в приложение D (Обработка на молби и жалби на физически лица, свързани с данни от ЕИП), когато отговарят на исканията на физически лица за достъп, коригиране и изтриване на лични данни.

2.1. Заявка за достъп

Администраторите на данни за ОЕ трябва да предоставят на лицата възможност да получат достъп при поискване до следното:

- Потвърждение дали Администраторът на данни разполага с Лични данни, свързани с тях
- Копие от личните им данни
- Целта (ите) на обработката
- Категориите лични данни, съхранявани за лицето;
- Получателите или категориите получатели, на които се разкриват Личните данни (особено получателите в страни извън ЕИП) и подходящите предпазни мерки, прилагани при такива прехвърляния;
- Където е възможно, периодът, за който ще се съхраняват Личните данни, или, ако не е възможно, критериите, използвани за определяне на този период;

- Съществуването на правото да се изисква от Администратора на данни коригиране или изтриване на лични данни или ограничаване на обработването на лични данни, отнасящи се до физическото лице, или да се възрази срещу такова обработване;
- Право на подаване на жалба до орган за защита на данните в ЕИП;
- Когато личните данни не се събират от физическото лице, всяка налична информация относно източника; и
- Съществуването на автоматизирано вземане на решения, включително профилиране, посочено в Глава D, Раздел V., и поне в тези случаи значима информация за съответната логика, както и значението и предвидените последици от такава обработка за лицето.

Администраторите на данни за ОЕ могат да отхвърлят такива заявки в случаите, изброени в приложение D ,Раздел V (Обработка на молби и жалби на физически лица, свързани с данни от ЕИП). Допълнителни изисквания за заявките за достъп са посочени във функционалното правило за обработка на заявки за достъп на субекти (SAR) и жалби за поверителност на данните (жалби).

2.2. Заявки за коригиране

Администраторите на данни за ОЕ трябва да предоставят на лицата възможността да изискат, без ненужно забавяне, коригиране на личните им данни (включително чрез предоставяне на допълнително изявление, отчитащо целите на обработването), което не отговаря на приложимите закони и разпоредби на ЕИП, по-специално защото е непълна или неточна.

Администраторите на данни за ОЕ могат да отхвърлят такива заявки в случаите, изброени в приложение D, раздел V. (Обработка на молби и жалби на физически лица, свързани с данни от ЕИП).

2.3. Заявки за заличаване

ОЕ администраторите на данни трябва да предоставят на физическите лица възможността да поискат заличаването на личните им данни, ако:

- Личните данни вече не са необходими във връзка с целите, за които са събрани или обработени по друг начин;
- Лицето оттегли съгласието, на което се основава Обработката, и няма друго законово основание за обработване;
- Индивидуалните възражения за Обработка, извършени въз основа на законните интереси на Администратора на данни, когато няма преобладаващи легитимни основания за Обработката, или

Индивидуалните обекти на Обработката за целите на директния маркетинг;

- Личните данни са обработени незаконно;
- Личните данни трябва да бъдат изтрити за съответствие с приложимите закони и разпоредби на ЕИП, на които Администраторът на данни е обект; или
- Личните данни се отнасят до дете или до физическо лице, чиито лични данни са били събрани, когато е било дете, както е определено съгласно приложимите закони и разпоредби на ЕИП, във връзка с предлагането на услуги на информационното общество.

Когато личните данни, предмет на искането за изтриване, са били публично оповестени от администратора на данни, той трябва да предприеме разумни стъпки, включително технически мерки, за да информира администраторите на данни, които обработват личните данни, за искането на физическото лице за изтриване на всякакви връзки към, или копия на тези Лични данни

Администраторите на данни за ОЕ могат да отхвърлят искането от лице за изтриване на неговите лични данни в случаите, изброени в приложение D, раздел V. (Обработка на молби и жалби на физически лица, свързани с данни от ЕИП). В такъв случай администраторите на данни за ОЕ могат да ограничат обработването на лични данни, предмет на искането за изтриване, ако допълнително бъде поискано от лицето в съответствие с глава D, раздел III.

II. Отговаряне на молбите на физически лица за възражение срещу обработване в ЕИП и трансфери на BCR

Администраторите на данни за ОЕ трябва да предоставят на лицата възможността да възразят по всяко време срещу обработването на техните лични данни, което се основава на законните интереси на администратора на данни, включително профилиране. В такъв случай администраторите на данни за ОЕ трябва да прекратят обработката на личните данни, освен ако не могат да посочат убедителни законни основания за продължаване на обработката, които отменят интересите, правата и свободите на лицето, или за установяване, упражняване или защита на правни претенции.

ОЕ администраторите на данни трябва да предоставят на лицата възможността да възразят по всяко време срещу обработването на техните лични данни за целите на директния маркетинг (включително профилиране, доколкото това е свързано с директен маркетинг). При упражняването на

това право от лицата, администраторите на данни за ОЕ трябва да прекратят обработката за целите на директния маркетинг.

Администраторите на данни за ОЕ трябва да се придържат към процедурата, посочена в приложение D (Обработка на молби и жалби на лицата, свързани с данни от ЕИП), когато отговарят на искания за възражения от физическо лице. Администраторите на данни за ОЕ могат да отхвърлят такива заявки в случаите, изброени в приложение D, раздел V.

III. Отговаряне на молбите на физически лица за ограничаване на обработването в ЕИП и BCR трансферите

1
3

Администраторите на данни за ОЕ трябва да предоставят на лицата възможността да ограничат обработката на техните лични данни и съответно личните им данни да бъдат разделени, ако:

- Точността на личните данни се оспорва от физическите лица за период, позволяващ на администратора на данни за ОЕ да провери точността на личните данни;
- Обработката е незаконна и лицата се противопоставят на изтриването на Личните данни и вместо това искат ограничаване на тяхната употреба;
- Администраторът на данни за ОЕ вече не се нуждае от лични данни за целите на обработването, но те се изискват от физическите лица за установяване, упражняване или защита на правни претенции; или
- Лицата са възразили срещу обработването, извършено въз основа на законните интереси на администратора на данни на ОЕ, в очакване на проверка дали законните основания на администратора заменят тези на лицата.

Когато обработката е ограничена, ОЕ администраторите на данни могат да обработват само лични данни, с изключение на съхранението:

- Със съгласието на лицето;
- За установяване, упражняване или защита на правни искове;
- За защита правата на друго физическо или юридическо лице; или
- По причини от важен обществен интерес, както са определени в приложимите закони и разпоредби на ЕИП.

Когато администратор на данни за ОЕ е ограничил обработването в отговор на искане на лице, той трябва да информира лицето за такова ограничение на обработката, преди то да бъде отменено.

Администраторите на данни за ОЕ трябва да се придържат към процедурата, посочена в приложение D (Обработка на молби и жалби на лица, свързани с данни от ЕИП), когато отговарят на искания за ограничение

от физически лица Администраторите на данни за ОЕ могат да отхвърлят такива заявки в случаите, изброени в приложение D, раздел V

IV. Отговаряне на исканията на физически лица за преносимост за обработка в ЕИП и BCR трансфери

Когато обработката се основава на съгласие или на договор и се извършва чрез автоматизирани средства, администраторите на данни за ОЕ трябва да дадат на физическите лица възможността да поискат:

- Получаването на предоставените от тях лични данни на ОЕ администратор на данни, в структуриран, често използван и машинно четим формат; и
- Предаването на неговите лични данни на друг администратор на данни без пречки от първоначалния администратор на данни на ОЕ, или за да предаване тези лични данни директно от един администратор на данни на друг, когато това е технически осъществимо

Администраторите на данни за ОЕ трябва да изпълнят искането на лицето за преносимост на неговите лични данни, при условие че това не засяга неблагоприятно правата и свободите на другите. Правото на лицето да поиска преносимост на неговите лични данни не засяга правото на лицето на заличаване.

Администраторите на данни за ОЕ трябва да се придържат към процедурата, посочена в приложение D (Обработка на заявки и жалби на лица, свързани с данни от ЕИП), когато отговарят на искания за преносимост на данни от физически лица. Администраторите на данни за ОЕ могат да отхвърлят такива заявки в случаите, изброени в приложение D, раздел V.

V. Отговаряне на исканията на физически лица за възражение срещу автоматизирани решения за обработка на ЕИП и трансфери на BCR

Администраторите на данни за ОЕ трябва да предоставят на лицата възможността да възразят срещу всяко решение, което води до правен ефект по отношение на това лице или което по друг начин значително засяга това лице, което се основава единствено на автоматизираната обработка на неговите лични данни, включително на базата на профилиране.

Администраторите на данни за ОЕ могат да отхвърлят такова искане, ако решението е:

- Необходимо за сключване или за изпълнение на договор между лицето и администратора на данни за ОЕ;

- Оторизирано от приложимите закони и разпоредби на ЕИП, на които се подчинява администратора на данни за ОЕ и които определят подходящи мерки за защита Правата и свободите на лицата и законни интереси; или
- Въз основа на изричното съгласие на лицето.

Администраторите на данни за ОЕ трябва да вземат решения само въз основа на автоматизираната обработка на чувствителните лични данни на лицата, при условие че са установили подходящи мерки за защита на правата, свободите и законните интереси на лицата, и:

- Лицето е дало своето изрично съгласие; или
- Обработката е необходима поради съображения от съществен обществен интерес, въз основа на приложимите закони и разпоредби на ЕИП

Администраторите на данни за ОЕ трябва да се придържат към процедурата, посочена в приложение D (Обработка на Искания и жалби на лица, свързани с данни от ЕИП), когато отговарят на възраженията на лицата срещу решения, които ги засягат въз основа на автоматизирана обработка, включително профилиране. Администраторите на данни за ОЕ могат да отхвърлят такива заявки в случаите, изброени в приложение D, раздел V.

E. Роли и отговорности

В настоящата глава са обобщени ролите и отговорностите на лицата, натоварени с дейностите по спазването на правилата, изложени в глави C и D. Допълнителна информация относно ролите и отговорностите са изложени във Функционалното правило за управление, мониторинг и гарантиране на неприкосновеността на личните данни.

I. На ниво Allianz Group

1.Управителният съвет на Allianz SE

Управителният съвет на Allianz SE носи цялостната отговорност за създаването на програма за защита на личните данни и защита на данните в Алианц Груп и осигуряване на съответствие с нея.

2. Group Privacy

Членът на управителния съвет на Allianz SE, отговарящ за бизнес подразделението H6, носи цялостната отговорност за Поверителността на Групата. На GP е възложена отговорност за разработването, ефективното прилагане и поддържане на програмата за поверителност и защита на данните в Allianz Group и трябва:

Консултира OE по всички теми, свързани със законите, регламентите, регулаторните указания, свързани с поверителността и защитата на данните, както и спазването им и трябва да поддържа и поддържа връзка с други функции по свързани теми;

Установява връзка с органи, регулатори, асоциации и други заинтересовани страни по въпроси, свързани с поверителността и защитата на данните;

Подготвя доклад за поверителността и защитата на данните, който ще се предоставя ежегодно от главния служител на Групата за поверителност на борда на Управителния съвет на Allianz SE, включително подробности за поверителността на данните и зрелостта на защитата в Allianz Group и всяко съществено несъответствие с Рамката;

Наблюдава изпълнението на OE и спазването на APS във връзка с други съответни функции на ниво Allianz Group или чрез независими прегледи, включително извършване на необходимите прегледи;

Поддържа и актуализира APS и уведомява OE за всякакви такива промени без ненужно забавяне, както и Физически лица, при поискване;

Поддържа база данни на ICA страните и уведомява OE за такива промени без ненужно забавяне, както и физически лица, при поискване;

Отчитайте ежегодно всички промени и актуализации на APS и ICA страните пред водещия орган за защита на данните на Allianz, Баварския орган за защита на данните (BayLDA), заедно с обосновки за такива промени и актуализации и, при необходимост, получавайте одобрение за всякакви съществени промени в APS;

Незабавно докладва на Баварския орган за защита на данните (BayLDA) всички промени, които биха могли да повлияят на нивото на защита, предлагана от Изискванията за BCRs трансфери, или значително да ги засегнат (напр. Промени в обвързващия характер); и

Свързва се с OE DPPs / DPOs относно правилното боравене с инциденти или нарушения на лични данни и упражняването на правата на лицата, посочени в глава D.

3. Group Chief Privacy Officer

Главният отговорник на Групата за поверителност („GCPO“) е ръководител на групата за поверителност на Allianz Група. GCPO се назначава от члена на управителния съвет на Allianz SE, отговарящ за бизнес подразделението H6.

GCPO трябва:

- Докладва директно на члена на Управителния съвет на Allianz SE с отговорност за бизнес отдел H6;
- Участва съгласно и своевременно във всички въпроси, свързани с поверителността и защитата на данните;
- Да има подходящи ресурси и неограничен достъп до дейностите по обработка;
- Поддържа своите експертни познания;
- Действа независимо (т.е. не получава никакви инструкции) по отношение на изпълнението на неговите / нейните задачи;
- Защитен е от уволнение или наказание при изпълнение на своите задачи;
- Обвързва се с тайна или поверителност относно изпълнението на своите задачи, в съответствие с приложимите закони и разпоредби на ЕИП;
- Изпълнява всякакви други задачи и задължения, при условие че не водят до конфликт на интереси (напр. GCPO не трябва да заема позиция, която да го кара да определя целите и средствата за обработка на лични данни);
- Публикува неговите / нейни данни за контакт и ги съобщавайте на водещия орган за защита на данните на Allianz, Баварския орган за защита на данните (BayLDA), и го уведомява за всички промени след това; и
- Да осигури достъп за физическите лица по всички въпроси, свързани с обработването на техните лични данни и упражняването на техните права.

GCPO е отговорен за надзора върху ефективното прилагане и поддържане на поверителността на личните данни и защитата на данните в Allianz Group и трябва да:

- Консултира и обучава Управителния съвет на Allianz SE по всички теми, свързани със законите, регламентите и регулаторните насоки за поверителност и защита на данните, както и спазването им;
- Консултира и обучава служители и друг персонал относно техните задължения и права съгласно APS;
- подготви и внедри инициативи за поверителност и защита на данните в цялата група;
- Наблюдава спазването на приложимите закони, разпоредби, регулаторни насоки и рамка за поверителност и защита на данните в Allianz Group;
- Свързва се с други функции на ниво Allianz Group относно правилното боравене с инциденти или нарушения на лични данни и относно упражняването на правата на физическите лица, посочени в глава D;
- Придържа се към процедурата за искания и жалби от физически лица, посочена в Приложение D (Обработка на молби и жалби на физически лица, свързани с данни от ЕИП), отправени към него/нея;
- Предоставя годишен доклад за поверителността и защитата на данните на Управителния съвет на Allianz SE, включващ подробности за поверителността на данните и зрялост на защитата в целия Allianz Group и всякакво съществено несъответствие с Рамката;
- Действа като звено за контакт и си сътрудничи с органите за защита на данните в ЕИП за всяко искане, свързано с Обработка на ЕИП, извършено на ниво група, включително предварителна консултация относно PIA или изискванията за прехвърляне на BCR;
- За ОЕ без регионална / глобална линия DPO действай съвместно с управителния съвет на ОЕ, за да:
    - Създаде и поддържа мрежа от DPP / DPO в групата Allianz
    - Установи функционални линии за отчитане от DPP / DPO до GCPO
    - Постави функционални цели за DPP / DPO по отношение на поверителността на данните и дейностите по защита;
    - Предостави устни и писмени оценки на изпълнението на DPP / DPO;
    - Предложи нива на компенсации и бонуси на DDP / DPO; и
    - Дава препоръки относно дисциплинарни процедури или прекратяване на договори с DPPs / DPOs.
- Въвежда и поддържа Консултативната група за защита на личните данни на Allianz („APAG“);
- По негова / нейната преценка, да се откаже изцяло или частично от всяко минимално глобално изискване за който и да е администратор на данни или обработващ данни извън ЕИП, за които не са приложими изискванията за обработка в ЕИП и изискванията за прехвърляне на BCR. GCPO трябва да документира писмено всяко изключение от

глобалните минимални изисквания и мотивите, подкрепящи това решение;

- Свързва се с DPPs / DPO на ОЕ и други съответни заинтересовани страни, за да:
  - Разрешава конфликт между разпоредбите на APS и местните закони и разпоредби; и
  - Докладва за всеки проблем на компетентните органи за защита на данните в ЕИП, произтичащ от закони и подзаконови актове, приложими за ОЕ извън ЕИП, които е вероятно да имат значителен неблагоприятен ефект върху гаранциите, предоставени в APS, включително, доколкото е позволено, всяка правно обвързваща искане за разкриване на данни от ЕИП от правоприлагащ орган или орган за държавна сигурност; и
- Застъпва се за интересите на Allianz Group относно поверителността и защитата на данните пред органите, регулаторите, асоциациите и други заинтересовани страни.

GCPO действа и като длъжностно лице за защита на данните („DPO“) за Allianz SE и за тази цел има директна функционална линия за докладване до члена на управителния съвет на Allianz SE, отговарящ за бизнес подразделението H6. При изпълнението на своите отговорности, GCPO трябва да вземе надлежно предвид рисковете, свързани с обработването, предприето от Allianz SE, като се има предвид естеството, обхвата, контекста и целите на обработката. Допълнителни изисквания относно двойната роля на GCPO като Allianz SE DPO са описани в съответното функционално правило за управление и наблюдение на поверителността.

II. Регионално ниво и глобални линии на Allianz

Регионите и глобалните линии трябва да посочат DPO за регионална / глобална линия. Регионалните / Global Line DPO отговарят за ефективното внедряване и поддържане на поверителността и защитата на данните в техния регион / Global Line, следят за спазването на приложимите закони за поверителност и защита на данните и рамката и информират и съветват служителите в техния регион / Глобална линия на техните задължения за защита на данните.

III. На ниво Allianz ОЕ

I.Управителен съвет на ОЕ

1.1. Глобални отговорности

Управителният съвет е отговорен за създаването и поддържането на стабилна и ясно дефинирана организационна и оперативна структура, за да гарантира спазването на Рамката, и трябва да:

- Осигури адекватни ресурси, обучение на персонала, водене на записи, качество на данните и ИТ системи и мониторинг;
- Осигури адекватен ресурс за спазване на процедурата за упражняване на правата на физическите лица, посочена в приложение D (Обработка на молби и жалби на физически лица, свързани с данни от ЕИП);
- Когато се изисква съгласно приложимите закони и наредби, назначава и получава предварителното одобрение на GCPO за длъжностно лице по защита на данните („DPO") или като специална длъжност, или като определена отговорност в рамките на съществуваща функция (например правна или функция за съответствие), че
  - Отговаря на изискванията на приложимите закони и наредби;
  - Притежава необходимите квалификации и опит, за да изпълни ролята на ДЛЗД, например, достатъчно разбиране на извършените операции по обработка, както и на информационните системи, сигурността и нуждите на личната информация и защитата на данните на ОЕ, включително посочените задължения в раздел 2 по-долу;
  - Има функционална и административна линия за докладване на член на борда на ОЕ, отговорен за поверителността и защитата на данните;
  - Може да действа независимо, с неограничен достъп до дейности по обработване и информация и без никакъв конфликт на интереси (т.е. DPO не трябва да заема позиция, която да го / я води да определя целите и средствата за обработка на лични данни); и
  - Участва в Консултативната група за защита на личните данни на Allianz („APAG") по искане на GCPO;
- Назначава професионалист за поверителност на данните („DPP"), когато приложимите закони и разпоредби не изискват назначаването на DPO и гарантират, че той / тя получават подходяща подкрепа и ресурси за изпълнение на своите задачи и задължения. Такива DPP:
  - Трябва да бъде подходящо квалифициран за изпълнение на задълженията, посочени в раздел 2 по-долу; и
  - Участва в APAG по искане на GCPO;
- Действа съвместно с GCPO или регионалната / глобална линейна DPO, според случая, за:
    - Предварително съгласуване относно назначаването на DPP / DPO;
    - Установяване на функционални линии за отчитане от DPP / DPO до GCPO

- Задаване функционални цели за DPP / DPO по отношение на поверителността на данните и дейностите по защита;
- Действа на всички устни или писмени оценки, направени от GCPO или регионалната / глобална линия DPO, според случая, на представянето на DPP / DPO;
- Задава нива на компенсация и бонус на DDP / DPO; и
- Дисциплинира или прекратяваDPP / DPO.

1.2. Допълнителни отговорности за обработка на ЕИП и прехвърляне на BCR

Управителният съвет на ОЕ трябва да определи длъжностно лице по защита на данните („DPO"), където:

- Основните дейности на ОЕ, действащи или като Администратор на данни, или като Обработващ Данни, се състоят от Обработка, която по своето естество, обхват и / или цел (и) изисква редовен и систематичен мониторинг на Лицата (напр. Пренасочване на имейл; маркетингови дейности; профилиране и отбелязване на резултатите за целите на оценката на риска (напр. кредитно точкуване, установяване на застрахователни премии, предотвратяване на измами, откриване на пране на пари); проследяване на местоположението; поведенческа реклама; мониторинг на уелнес, фитнес и здравни данни чрез носими устройства; свързани устройства (напр. интелигентни измервателни уреди, интелигентни автомобили, домашна автоматизация) в голям мащаб (напр. Обработка на лични данни на клиента за установяване на застрахователни премии);
- Основните дейности на ОЕ, действащи като администратор на данни или като обработващ данни, се състоят от обработка в голям мащаб на чувствителни лични данни и лични данни, свързани с наказателни присъди и престъпления (вж. Глава В, раздели IV.2- 2.2. И 2.3.); или
- Това се изисква от приложимите закони и разпоредби

Когато преценява дали DPO трябва да бъде назначен, както е описано по-горе, управителният съвет на ОЕ трябва да документира такава оценка, за да докаже, че съответните фактори са били правилно взети предвид. Такава оценка трябва да се извърши, когато е необходимо (например, ако ОЕ предприема нови дейности или предоставя нови услуги, които биха могли да отговорят на горните критерии).

Управителният съвет на ОЕ трябва да гарантира, че DPO:

Се назначава в съответствие с приложимите закони и разпоредби на ЕИП и / или изискванията на органите за защита на данните в ЕИП от време на време;

Има директни функционални и административни линии за докладване до управителния съвет на ОЕ;

Участва, правилно и своевременно, във всички въпроси, свързани с поверителността и защитата на данните, т.е. Всяко отклонение от неговия / нейния съвет трябва да бъде документирано;

Има подходящи ресурси, неограничен достъп до дейности по обработка и поддържа своите експертни познания;

Действа независимо (не получава никакви инструкции) по отношение на изпълнението на тези задачи;

Защитен е от уволнение или наказание при изпълнение на задачите си;

Обвързан е с тайна или поверителност относно изпълнението на задачите си в съответствие с приложимите закони и разпоредби на ЕИП;

Изпълнява всякакви други задачи и задължения, при условие че не водят до конфликт на интереси (напр. DPO не трябва да заема позиция в ОЕ, водеща до определяне целите и средствата за обработка на лични данни);

Публикува неговите / нейните данни за контакт, съобщава неговото / нейното име и данни за контакт на органа за защита на данните в ЕИП, компетентен за ОЕ, и уведомява този орган за защита на данните за всички промени след това; и

Осигурен е достъп до тях за физически лица (напр. Да се намират в ЕС, където е подходящо) по всички въпроси, свързани с обработването на техните лични данни и упражняването на техните права.

2.Професионален служител за защита на личните данни на ОЕ / Служител по защита на данните / OE Data Privacy Professional/Data Protection Officer

2.1 Глобални отговорности

Професионалистът за поверителност на данните на ОЕ („DPP“) / длъжностно лице по защита на данните („DPO“) трябва да:

- Осигурява подходящо прилагане на Рамката на ниво ОЕ;

- Съгласува техните функционални дейности с цели и директиви, определени съвместно от управителния съвет на ОЕ и GCPO;

- Наблюдава спазването на приложимите закони, регламенти, регулаторни насоки и рамка в ОЕ за поверителност и защита на данните;

- Потвърждава, че процесите за поверителност на данните и свързаните със защитата процеси се прилагат по подходящ начин, поддържат и спазват в съответствие със съответните вътрешни и външни изисквания;

- По указание на GCPO докладва резултатите от дейностите по мониторинг, по-специално, съществуването на съществени недостатъци на поверителността и защитата на данните от ОЕ;

- Консултира служителите относно техните задължения и права съгласно рамката, включително чрез провеждане или осигуряване на обучение по поверителност и защита на данните;

- отчита надлежно при изпълнението на своите отговорности риска, свързан с обработката, като се има предвид естеството, обхватът, контекстът и целта (ите) на обработката;

- Изпълнява задачите и задълженията, посочени в раздел II.3. по-долу, освен ако той / тя не реши да делегира някои от тях на специалиста (ите) за поверителност на ОЕ, назначен (и) от управителния съвет на ОЕ, в този случай ОЕ DPP / DPO запазва отговорността за надзор върху дейностите на специалистта по поверителност;

- Съставя и запазва запис на задачите и задълженията, които той / тя е възложил на специалистта(ите) за поверителност на ОЕ;

- Когато е приложимо, незабавно информира GP (или улеснява уведомяването на GP чрез функцията за поверителност на регионалните / глобалните линии, където е приложимо) за всеки потвърден или потенциално съществен инцидент с лични данни, в съответствие с изискванията за докладване, посочени във функционалното правило за лични данни Управление на инциденти;

- Свързва се с GCPO или GP за:
    - Разрешаване на всякакви противоречия между разпоредбите на APS и местните закони и разпоредби;
    - Докладва за всеки проблем на компетентните органи за защита на данните, произтичащ от закони и подзаконови актове, приложими за ОЕ извън ЕИП, които има вероятност да окажат значително неблагоприятно въздействие върху гаранциите, предоставени в APS, включително, доколкото е позволено, всяко правно обвързващо искане за разкриване на данни от ЕИП от правоприлагащ орган или орган за държавна сигурност;
    - да се изясни обхватът или приложението на която и да е част от рамката; и

- Свързва се с местните органи за защита на данните, регулатори и органи; и
- Сътрудничи с GCPO и / или други оригинални организации за обработка на искане или жалба от физическо лице или в отговор на разследване или запитване от който и да е орган за защита на данните.

Всяко споразумение между ОЕ и трета страна или компания Allianz Group, чрез което тази трета страна или компания Allianz Group изпълнява някоя от отговорностите на DPP / DPO, която се квалифицира като аутсорсинг по смисъла на Политиката за аутсорсинг на Allianz Group (или се прилага на местно ниво) еквивалент на това), се подчинява на изискванията на политиката за аутсорсинг на Allianz Group или съответната местна политика на аутсорсинг

2.2 Допълнителни отговорности за обработката на ЕИП и трансферите на BCR

ОЕ DPP / DPO трябва:

- В случай на нарушение на личните данни, да спазва приложимите законови и регулаторни изисквания, както и изискванията, съдържащи се във Функционалното правило за управление на инциденти с лични данни, Стандартът на Allianz за защита и устойчивост (AZ P&R

Standard), Функционалното правило на Allianz за защита и устойчивост (AZ P&R функционално правило), директивите на Allianz за информационна сигурност (AISD) и всякакви други приложими политики на Allianz;

- Да си сътрудничи и да се придържа към съветите на който и да е орган за защита на данните в ЕИП относно тълкуването на изискванията за прехвърляне на BCR;

- Да оцени всяко решение или решение, взето от съд, трибунал или административен орган извън ЕИП, изискващи прехвърляне или разкриване на данни от ЕИП, и да се консултира с ОЕ или външен юрисконсулт, за да се увери, че такова прехвърляне или разкриване се извършва в съответствие с приложими закони и разпоредби на ЕИП;

- В случай на правно обвързващо искане за разкриване на данни от ЕИП от правоприлагащ орган или орган за държавна сигурност:

    - Свързва се с GCPO или GP, веднага щом ОЕ узнае, че правоприлагащ орган или орган за държавна сигурност обмисля да поиска разкриване на данни от ЕИП;

    - Доколкото е позволено, подава молба на задържане за разумен период преди всяко разкриване на запитващия орган или орган, за да я докладвате на компетентните органи за защита на данните в ЕИП. Информацията, предоставена на компетентните органи за защита на данните в ЕИП, трябва да включва информация за поисканите данни за ЕИП, органа или органа, който е поискал, и правното основание за разкриването;

    - Когато искането не може да бъде спряно или уведомяването на компетентните органи за защита на данните в ЕИП е забранено, използвай и демонстрирай най-добрите усилия за получаване на правото да се откажете от тази забрана, за да предаде възможно най-много информация на компетентните органи за защита на данните в ЕИП, възможно най-скоро;

    - Когато не се разрешава отказ от забраната или не се получава разрешение за уведомяване на компетентните органи за защита на данните в ЕИП, ежегодно предоставяй на компетентните

органи за защита на данните обща информация за всички получени искания (напр. брой заявления за разкриване, вид на заявените данни за ЕИП). , подробности за заявителя, ако е възможно и т.н.); и

- Не извършва никакви трансфери на данни от ЕИП на нито един молещ правоприлагащ орган или орган за държавна сигурност, които са масивни, непропорционални и безразборни по начин, който надхвърля необходимото в демократичното общество;

➢ Периодично преглежда Изискванията за прехвърляне на BCR в съответствие с приложимите закони и разпоредби, които могат да попречат на ОЕ да изпълни задълженията си по Рамката, и да се свържете с GCPO или GP за:

- Разрешава всякакви противоречия между разпоредбите на APS и местните закони и разпоредби и информира всички съответни заинтересовани страни;

- Докладвайте за всеки проблем на компетентните органи за защита на данните в ЕИП, произтичащ от закони и подзаконови актове, приложими за ОЕ извън ЕИП, които е вероятно да имат значителен неблагоприятен ефект върху гаранциите, предоставени в APS; и

➢ Сътрудничи и действа като контактна точка за компетентните органи за защита на данните в ЕИП по въпроси, свързани с Обработката в ЕИП, извършена на ниво ОЕ, включително предварителна консултация по PIAs.

3.ОЕ Специалисти по поверителността

Администраторите на данни на ОЕ и обработващите данни на ОЕ, в сътрудничество с ОЕ DPP / DPO, трябва да назначат един или повече Специалист (и) по поверителността като определена отговорност в рамките на съществуващите бизнес функции, както е подходящо въз основа на критерии, предоставени от GP, и да гарантират, че на специалистите се предоставя подкрепа и ресурси, необходими за изпълнение на възложените им задачи и задължения

3.1 Глобални отговорности

Allianz

Специалиста по поверителност на ОЕ действа като комуникационен канал между бизнес функциите на ОЕ и ОЕ DPP / DPO и освен ако не е указано друго от ОЕ DPP / DPO, трябва:

- Да осигури подходящо прилагане на Рамката през ОЕ по посока на ОЕ DPP / DPO;
- Подпомага прилагането, поддръжката и спазването на процесите за поверителност на данните и свързани със защитата в съответствие с Рамката;
- Подкрепя ОЕ за спазване на изискванията за поверителност и защита на данните и своевременно потърсете съвет от ОЕ DPP / DPO, когато е подходящо;
- Насърчава и доставя ключови съобщения за поверителност и защита на данните и подпомагайте ОЕ DPP / DPO с подготовката и доставката на обучение за поверителност и защита на данните, осведоменост и комуникационни инициативи;
- Създава и поддържа дневници на текущи, отворени и разрешени молби и жалби и жалби, свързани с поверителността на данните и жалби от физически лица, запитвания от вътрешни и външни заинтересовани страни и предприети проблеми и действия; и да предостави такива регистрационни файлове на ОЕ DPP / DPO при поискване;
- Координира докладването на нарушения на личните данни на ОЕ DPP / DPO;
- Консултира бизнес функциите на ОЕ и ОЕ DPP / DPO относно това дали трябва да бъдат завършени PIA за процеси или процедури, които представляват нисък или среден риск за поверителност и защита на данните;
- Подпомага бизнес функциите на ОЕ за създаване и поддържане на записи на дейностите по обработка, въз основа на информацията, предоставена от Собственика на информацията и в съответствие с Функционалното правило за оценка на въздействието върху поверителността (PIA) и записи на обработката; и
- Сътрудничи с ОЕ DPP / DPO, GCPO или други ОЕ, за да обработи искане или жалба от физическо лице или в отговор на разследване или запитване от който и да е орган за защита на данните.

3.2 Допълнителни отговорности за обработка на ЕИП и прехвърляне на BCR

Специалистът по поверителност на ОЕ, освен ако не е указано друго от ОЕ DPP / DPO, трябва:

- Да извършва независима обработка на искания от физически лица, свързани с техните права, посочени в глава D, както и жалби от физически лица, свързани с прехвърляния на BCR, в съответствие с процедурата, посочена в приложение D (Обработка на молби и жалби на физически лица, свързани с данни от ЕИП); и
- Незабавно да информира ОЕ DPP / DPO за резултата от искания и жалби от физически лица.

4. Собственик на информация за ОЕ

Собствеността на лични данни за целите на рамката е свързана с професионалната и бизнес отговорност на организационна единица за конкретна дейност по обработка на данни. Организационната единица, която създава или инициира създаването или съхранението на Лични данни, представлява собственикът на тези Лични данни и се представлява от физическото лице в бизнеса, което в крайна сметка отговаря за Дейността по обработване („Собственик на информация"). Собственикът на информацията трябва, доколкото се отнася до сферата на отговорност на собственика на информация:

Да осигури спазване на изискванията на Рамката;

Да се увери, че личните данни се събират и обработват само дотолкова, доколкото е необходимо да се изпълни определена, изрична и законна бизнес цел;

Да се увери, че функционалната отговорност на собствеността върху личните данни е ясно определена и документирана и че тези лични данни са адекватно идентифицирани и класифицирани в съответствие с Рамката за информационна сигурност на Allianz Group (GISF); и

Да се увери, че адекватните и конкретни контроли за поверителност и защита на данните са дефинирани и приложени по време на жизнения цикъл на Личните данни (обхващащи тяхното събиране или създаване, съхранение, обработка, прехвърляне и унищожаване), и редовно да преглежда тези контроли за целесъобразност и ефективност в съответствие с Рамката за информационна сигурност на Allianz Group (GISF).

3. Allianz Group и OE Steering

1. Allianz Общност за поверителност и защита на данните

OEP DPPs / DPOs и Privacy Champions са част от глобалната общност на Allianz за поверителност и защита на данните. Общността за поверителност и защита на данните се ръководи и координира от GP, за да се осигури цялостно покритие на поверителността и защитата на данните в Allianz Group.

2. Консултативна група за поверителност на Allianz

OE, регионите и глобалните линии трябва да бъдат представени в Allianz Privacy Advisory Група („APAG"). Целта и съставът на APAG са допълнително описани в Техническото задание на Allianz Privacy Advisory Group (APAG), изменяно от време на време

F. Препратки

APS представлява част от рамката за поверителност и защита на данните на Allianz („Рамка"). Рамката включва следното, изменяно от време на време:

- ФП за оценка на въздействието върху поверителността и етиката и регистрите за обработка (Functional Rule for Privacy Impact & Ethics Assessments and Records of Processing)
- ФП за управление на запитванията от субекти и жалбите (Functional Rule for the handling of Subject Access Requests (SARs) and Data Privacy Complaints)
- ФП за управление на инциденти с лични данни (Functional Rule for Personal Data Incident Management)
- ФП за управление, мониторинг и осигуряване на поверителност (Functional Rule for Privacy Governance, Monitoring and Assurance)
- В допълнение, Рамката се допълва от следните, изменяни от време на време:
  - Рамката на Алианц за информационна сигурност (Allianz Group Information Security Framework (GISF), която се състои от:

o Политиката на Алианц за информационни технологии и информационна сигурност (Allianz Group Information Technology and Information Security Policy
(APITIS)

- ФП за информационна сигурност (Allianz Functional Rule for Information Security (AFRIS)
- ФП за управление на информационния риск (Allianz Functional Rule for Information Risk Management (AFIRM)
- Практиките на Алианц за информационна сигурност (Allianz Information Security Practices)

- Стандарта на Алианц за управление на информацията и документите (Allianz Standard for Information and Document Management (ASIDM)
- Стандарта на Алианц за защита и устойчивост (Allianz Standard for Protection & Resilience (AZ P&R Standard)
- ФП за защита и устойчивост (Allianz Functional Rule for Protection & Resilience (AZ P&R Functional Rule)

Допълнителна информация е достъпна чрез Allianz Connect в Корпоративния правилник.

Приложение А: Речник

Term	Описание
Allianz Group	Allianz SE и неговите дъщерни дружества (вж. Годишен доклад, речник, термин „свързани предприятия"), с изключение на асоциирани предприятия, съвместни предприятия (освен ако Group Privacy не е направил официална преценка за приложимост по отношение на такъв субект или както е изрично посочено в споразумението за съвместно предприятие) и холдингови компании без оперативна или стратегическа функция, но включително Групи (т.е. организационна единица за бизнес сегмент или бизнес в регион, която е организирана с отделен холдинг, контролиращ дъщерните дружества и определящ стандарти за тях) и организационни единици като Allianz Re.

APAG	Консултативната група за защита на личните данни на Allianz, консултантски и ръководен орган, създаден с цел подпомагане на поддържането на устойчиво ниво на поверителност и защита на данните в рамките на Allianz Group чрез разработване и прилагане на дейности, проекти и инициативи за защита на личните данни и защита на данните.
Обвързващи корпоративни правила или BCR **Binding Corporate Rules or BCRs**	Законно признат механизъм за легитимиране и улесняване на трансфери на лични данни, произхождащи от или обработени в ЕИП в рамките на корпоративна група.
BCRs Transfers	Разкриване на данни от ЕИП чрез физическо предаване или отдалечен достъп до ОЕ, които не са членки на ЕИП, които са страна по ICA.
Администратор на данни - Data Controller	Физическо или юридическо лице, публичен орган, агенция или друг орган, който сам или съвместно с други определя целите („защо“) и средствата („как“) за обработване на лични данни. В случай че двама или повече администратори на данни определят съвместно целите и средствата за обработка, те се считат за съвместни администратори и трябва да си сътрудничат по прозрачен начин, за да осигурят спазването на рамката.
Обработващ данни -Data Processor	Физическо или юридическо лице, което обработва лични данни от името на администратор на данни.
ЕИП - EEA	Страните, които са образуваща част от Европейския съюз, както и Исландия, Лихтенщайн и Норвегия.ЕИП-Европейско Икономическо Пространство
ЕИП данни - EEA Data	Лични данни, чиято обработка се подчинява на законите и разпоредбите на ЕИП.
ЕИП Обработка EEA Processing	Обработката на данни от ЕИП, когато: ✦ Личните данни се обработват в контекста на дейностите на Администратор на данни или установяване на Обработващия Данни в ЕИП, дори ако самата Обработка не се извършва в ЕИП; или

	✦ Личните данни на физически лица, които са в ЕИП, се обработват за предлагане на стоки или услуги на физически лица или за наблюдение на тяхното поведение.
Служители Employees	Служители на ОЕ (включително всички работници на пълен работен ден, на непълно работно време, временни и случайни работници; консултанти, изпълнители и временни работници; стажанти и студенти с трудов опит), мениджъри, директори и членове на изпълнителния съвет.

Рамка Framework	Стандартът за поверителност на Allianz („APS“) и неговите функционални правила, изброени в глава F. Препратки.
Глобална линия **Global Line**	Бизнес линии, които се управляват в световен мащаб, а не на местно или регионално ниво, напр. AGCS или Euler Hermes.
Главен отговорник на групата за поверителност или GCPO **Group Chief Privacy Officer or GCPO**	Ръководителят на Group Privacy на Allianz Group, назначен от Управителния съвет на Allianz SE.
Group Privacy or GP	Отделът за поверителност на групите в Allianz SE.
Лице/субектна лични данни-Individual	Идентифицирано или идентифицируемо лице, за което се отнасят Личните данни. Подлежащо на идентификация физическо лице е това, което може да бъде идентифицирано, пряко или косвено, по-специално чрез позоваване на идентификатор като име, идентификационен номер, данни за местоположението, онлайн идентификатор или на един или повече фактори, специфични за физическите, физиологичните, генетичните , психическа, икономическа, културна или социална идентичност на това физическо лице. В Рамката той се отнася до

	служители и свързания с тях персонал, клиенти, бизнес партньори или други трети страни, чиито лични данни се обработват, както е описано по-нататък в приложение B.
Собственик на информация **Information Owner**	Служебно лице, което може да включва собственик на документ, както е дефиниран в ASIDM, или бизнес собственик на бизнес приложение, както е дефинирано в AFRIS, в крайна сметка отговорен за дейността по обработка на лични данни в организационната единица, която създава или инициира създаването или съхранението на лични данни.
Вътрешнофирмено споразумение /Intra-Company Agreement or ICA	Вътрешнофирменото споразумение за прилагане на BCR на Allianz, подписано от юридически лица в рамките на Allianz Group, за да даде правно действие на APS.
OE	Управляващ субект в рамките на бизнес сегмент, независимо от неговата правна форма (и който е под контрола на Allianz съгласно Закона за германските акционерни дружества), с изключение на асоциирани предприятия и съвместни предприятия (освен ако Group Privacy не е направила официална преценка за приложимостта на такова предприятие или както е изрично посочено в споразумението за съвместно предприятие). OE може да се състои от едно или повече юридически лица или, обратно, едно юридическо лице може да се състои от две OE (например в случай на композити). Позоваването на OE включва препратка към всички юридически лица и клонове, които са част от това OE.
Специалисти по поверителността Privacy Champions	Лицата с определена отговорност в рамките на съществуващите бизнес функции на OE, които действат като комуникационен канал между OE бизнес функциите и OE DPP / DPO, и поддържа OE бизнес функцията с теми, свързани с поверителността и спазване на защитата на данните, както е указано

	от ОЕ DPP / DPO или както е делегирано от Собственика на информацията.
Лични данни Personal Data	Всякаква информация, свързана с физическо лице.
Нарушаване на личните данни Personal Data Breach	Означава нарушение на сигурността, водещо до случайно или незаконно унищожаване, загуба, изменение, компрометиране, неразрешено разкриване или достъп до лични данни, предавани, съхранявани или обработвани по друг начин от или от името на Allianz, и което поражда регулаторни задължения.
Инциденти с лични данни Personal Data Incident	Събитие, което включва или би могло да включва лични данни и което има потенциал да се превърне в нарушение на личните данни.
	За целите на APS инцидентът с лични данни може да се отнася и до потенциално нарушение на личните данни.
Privacy Impact & Ethics Assessment or PIA	
Структуриран и повторяем анализ на инициативи и съществуващи или планирани промени, засягащи бизнес процеси, процедури, системи, продукти или услуги, включващи Обработката на лични данни. Този анализ предоставя информация за идентифициране, **Оценка и въздействие върху поверителността** и смекчаване на рисковете за поверителност и защита на данните, включително тези, произтичащи от **оценка на етиката** от използването на изкуствен интелект при обработка на лични данни или **PIA** дейности, и описва адекватни и пропорционални мерки за намаляване на въздействието и вероятността на рисковете за поверителност и защита на данните, включително технически и организационни мерки (например регламенти, процедури, насоки, правни договори, управленски практики или организационни структури).	
Обработка/ Processing	Всяка операция или набор от операции, извършени върху Лични данни или върху набори от Лични данни,

независимо дали чрез автоматизирани средства, като събиране, запис, организация, структуриране, съхранение, адаптация или промяна, извличане, консултация, използване, разкриване чрез предаване, разпространение или предоставяне по друг начин, подравняване или комбинация, ограничаване, изтриване или унищожаване.

Профилиране/ Profiling Всяка форма на автоматизирано обработване на лични данни, състояща се от използване на лични данни за оценка на определени лични аспекти, свързани с физическо лице, по-специално за анализ или прогнозиране на аспекти относно изпълнението на това лице на работа, икономическа ситуация, здраве, лични предпочитания, интереси, надеждност, поведение, местоположение или движения.

Subject Access Requests or SARs

Упражняването от физическите лица на правото им на заявка за достъп, свързано с обработването на личните им данни от субекта, както е предвидено в приложимите закони и подзаконови актове за заявки или SAR, и обхванати в глава D, раздел I; 2.1.

Sensitive Personal Data

/Чувствителни лични данни

Лични данни, разкриващи расов или етнически произход, политически мнения, религиозни или философски убеждения или членство в профсъюзи, и Обработка на генетични данни, биометрични данни с цел еднозначно идентифициране на физическо лице, данни относно здравето или данни относно сексуалния живот или сексуалния живот на физическо лице ориентация. ичните данни, които по своето естество могат потенциално да представляват по-висок риск за неприкосновеността на личния живот и правата и свободите на лицата, но не са включени тук, са известни като „Други чувствителни лични данни" (напр. Данни за банкова сметка, заплата, данни за документ за самоличност) , подписи). Чувствителните лични данни и други чувствителни лични данни изискват по-високо ниво на защита от личните данни (напр. Съгласие, криптиране).

Приложение Б: Трансфери съгласно Задължителни корпоративни правила (BCRs), обхванати от APS [1]

I. Категории лица

Изискванията за BCR трансфери обхващат следните категории лица:

- Настоящи, бивши и бъдещи служители, включително, но не само, на пълно работно време, на непълно работно време, временни и случайни работници; работници на заплата, консултанти, изпълнители и временни работници; стажанти и студенти с трудов опит; кандидати; и отношения на служителите („HR данни").

- Настоящи, бивши и бъдещи клиенти, корпоративни клиенти, представители на клиенти и корпоративни клиенти и други трети страни (напр. Ищци, бенефициенти, жалбоподатели, запитващи, пенсионни членове и бенефициенти) („Данни на клиента").

- Настоящи, бивши и бъдещи агенти, брокери, посредници; доставчици и доставчици на услуги; пенсионни настоятели; акционери; и всички други бизнес партньори („Данни на трети страни").

II. Категории лични данни

Изискванията за BCR трансфери обхващат следните категории лични данни:

- **HR данни**: включително, но не само, основни лични данни (напр. Пълно име; възраст и дата на раждане); образование, професионален опит и принадлежности (напр. история на образование и обучение; езици; членство в синдикати); информация за пътуването и разходите на служителите (напр. данни за резервация на пътуване; диетични изисквания; данни за паспорт и виза); семейство, начин на живот и социални обстоятелства (напр. семейно положение; данни за спешен контакт; религия или религиозни вярвания); основни данни за човешките ресурси (напр. длъжност, роля; местоположение на офиса; начална дата); свързани със здравето, благосъстоянието и отсъствието (напр. причина за отсъствие; увреждане, достъп, подробности за специални

изисквания); свързано с изпълнението на служителите (напр. дисциплинарно наказание, оценка на изпълнението); финансови данни (напр. информация за банкова сметка; национален осигурителен номер; бонусни плащания); информация за фотография, видео и местоположение (напр. изображения за видеонаблюдение; данни за проследяване); проверки за идентификация и проверка на миналото (напр. резултати от криминални проверки; доказателство за допустимост за работа);

- **Данни на клиента**: включително, но не само, основни лични данни (напр. Пълно име, възраст и дата на раждане); бизнес дейности (напр. предоставени услуги); семейство, начин на живот и социални обстоятелства (напр. лица на издръжка, съпруг, партньор, семейни данни; религия или религиозни убеждения; наказателни присъди и престъпления); свързани със здравето, благосъстоянието и отсъствието (напр. подробности за физическото и психологическото здраве или медицинско състояние; оплаквания и оплаквания); финансови данни (напр. информация за банкова сметка; национален осигурителен номер); информация за фотография, видео и местоположение (например изображения за видеонаблюдение); проверки за самоличност и проверка на миналото (напр. резултати от криминални проверки; свързани с проверка на кредитоспособността).;
- **Данни на трети страни**: включително, но не само, основни лични данни (напр. Пълно име); стопански дейности (напр. стоки или услуги); финансови данни (напр. информация за банкова сметка); информация за фотография, видео и местоположение (например изображения за видеонаблюдение); проверки за идентификация и проверка на миналото (напр. резултати от криминални проверки).

III. Цели на обработката

Изискванията за BCR трансфери обхващат всякакъв вид обработка и следните цели:

- **Данни за човешките ресурси**: управление на човешките ресурси, включително, но не само, общо администриране на трудовото правоотношение (напр. Работна заплата), набиране на персонал, управление на таланти, обучение и развитие на персонала (напр. Обучение), безопасност и сигурност, управление на стимулите, превенция на професионалните рискове (т.е. свързани със

здравето, работата и околната среда), управление на ИТ услуги за поддръжка; трудови правоотношения (например взаимоотношения със работнически съвет); управление на вътрешни дейности за подпомагане (напр. правен; вътрешен одит); управление на непрекъснатостта на бизнеса (например непрекъснатост и планиране и реакция при кризи); и спазване на законовите задължения (например подаване на сигнали за нередности).;

- **Клиентски данни**: управление на взаимоотношенията с клиенти, включително, но не само, продажби и обслужване на клиенти, фактуриране, маркетинг, комуникация, данъци, управление на ИТ, обработка на жалби; обработка на застрахователни искове; обработка на искове за здравно и животозастраховане; администриране на финансирани пенсии или пенсионни схеми; управление на портфейлни активи; управление на собствеността; операции; управление на вътрешни дейности за подпомагане (напр. правен; вътрешен одит); отчитане; спазване на законовите задължения (напр. борба с изпирането на пари); и безопасност и сигурност.;
- **Данни на трети страни**: управление на партньорски отношения, включително, но не само, управление на договори за агент, администриране на капиталови пенсии или схеми за пенсионно осигуряване, управление на ИТ, управление на стимули; управление на вътрешни дейности за подпомагане (напр. правен; вътрешен одит); администрация и вътрешно отчитане; и безопасност и сигурност.

Приложение C: Минимални изисквания за договорните отношения между Администратор на данни и Обработващ данни за обработка в ЕИП и прехвърляне съгласно ЗКП (BCR) 2 3

I. Обработващи данни, които не са ОЕ

За обработки на данни в ЕИП и трансфери съгласно BCR, администраторите на данни за ОЕ трябва да включват следните изисквания при сключване на договори с обработващи данни, които не са ОЕ, съгласно Глава В, раздел V.2.

Разпоредби, свързани с обработването в ЕИП:

- ✓ Предмет и продължителност на обработката;
- ✓ Същност и цел на обработката; и

Тип лични данни и категории физически лица

Задължения и права на администратора на данни за ОЕ

✓ Задължения на администратора на данни за ОЕ; и

✓ Права на администратора на данни за ОЕ

Ангажименти на обработващия данни:

Обработва лични данни само по документирани инструкции от администратора на данни за ОЕ, включително за прехвърляне в страни извън ЕИП;

Докладва за всички закони и разпоредби на ЕИП, приложими за обработващия данни, които изискват от него да обработва личните данни извън обхвата на инструкциите на администратора на данни на ОЕ, освен ако такава информация е забранена поради важни основания от обществен интерес;

Уверява се, че разрешенията за обработка на лични данни са дадени само на лица, обвързани с ангажимент за поверителност или подходящо законово задължение за поверителност;

Взема всички необходими мерки за сигурност, така че Обработката да отговаря на изискванията, посочени в глава Б, раздел VII.2 .;

Ангажира под-обработващите само с предварително конкретно или общо писмено разрешение на администратора на данни на ОЕ;

Ако генералното писмено разрешение е дадено от администратора на данни за ОЕ, информира Администратора на данни за ОЕ на всички предвидени промени, свързани с добавянето или подмяната на Обработващите, заедно с възможността да възразят срещу подобни промени;

Прехвърля задълженията си за поверителност и защита на данните на под-обработващи лица чрез договор или друг правен акт, без да се освобождава от отговорността си към администратора на данни на ОЕ, включително за всяко нарушение или неизправност от под-обработващите;

Подпомага на администратора на данни на ОЕ чрез подходящи технически и организационни мерки, като се отчита естеството на обработката и доколкото това е възможно, за изпълнението на задължението на

администратора на данни на ОЕ да отговаря на искания за упражняване на правата на физическите лица;

Подпомага на администратора на данни за ОЕ при осигуряване на спазването на неговите задължения, свързани със сигурността, уведомяване за нарушения на личните данни на органите за защита на данните в ЕИП и / или на физическите лица, и PIA, като се вземе предвид естеството на обработването и информацията, с която разполага обработващият данни;

По избор на администратора на данни на ОЕ изтрива или връща всички лични данни администратора на данни на ОЕ в края на предоставянето на каквито и да било услуги, свързани с Обработката, и изтрива съществуващи копия, освен ако приложимите закони и разпоредби на ЕИП изискват съхранение на личните данни ; и

Предоставя на разположение на администратора на данни на ОЕ цялата информация, необходима за доказване на спазването на неговите задължения съгласно приложимите закони и разпоредби на ЕИП и разрешаване и участие в одити, включително инспекции, проведени от администратора на данни на ОЕ или друг одитор, упълномощен от администратора на данни за ОЕ; и незабавно информира администратора на данни за ОЕ, ако според него инструкцията нарушава приложимите закони и разпоредби на ЕИП

II. Обработващи данни за ОЕ

По подразбиране изискванията на APS се отнасят както за ОЕ, действащи като администратори на данни, така и за ОЕ, действащи като обработващи данни от името на ОЕ администраторите, освен ако не е посочено друго. Освен това, когато Изискванията за обработка на ЕИП и BCR прехвърляния се отнасят само за ОЕ администраторите на данни, ОЕ обработващите данни трябва да се придържат към стандартите, наложени на тези ОЕ администратори на данни, и да улесняват способността на ОЕ администраторите на данни да се съобразяват с тези стандарти.

Освен това администраторите на данни за ОЕ, сключващи договори с обработващите данни за ОЕ, са обвързани заедно с разпоредбите на Условията за вътрешнофирмена обработка на данни, приложени в Приложение 1 към настоящото приложение С; разбира се, че администраторите на данни за ОЕ и обработващите данни за ОЕ трябва да попълнят Бланкабланките, посочени в приложения 1, 2 и 3; и попълнените документи трябва да се обменят между съответния администратор на данни за ОЕ и съответния обработващ данни за ОЕ във всеки отделен случай и да

бъдат приложени към отделното писмено споразумение, което трябва да бъде сключено преди обработката, според случая.

Освен това се прилагат условията във връзка с обработката в ЕИП и прехвърлянето съгласно BCR, съгласно глава B, раздел V.2 от APS.

Приложение 1 към приложение B: Условия за обработка на

вътрешнофирмени данни

между

[Име и адрес на данните, обект на контролиране от Allianz]

"Администратор на данни"

и

[Име и адрес на данните, обект на обработване от Allianz]

"Обработващ данни"

Преамбюл

Настоящите Условия за обработка на данни в рамките на компанията („Условия за DP") се прилагат за всички ОЕ на Allianz Group, които са сключили Вътрешнофирменото споразумение за прилагане на

Обвързващите корпоративни правила на Allianz или се позовават изрично на Стандарта за поверителност на Allianz в отделно писмено споразумение, свързано с предоставянето на услуги от обработващия лични данни, което трябва да бъде сключено преди обработката („Споразумение“) и при обработката на лични данни (вътрешногрупова обработка), независимо дали отделният ОЕ действа като администратор на данни или съответно като обработващ данни.

За всяка отделна обработка приложенията от 1 до 3 се попълват индивидуално в писмена форма и се прилагат към споразумението, според случая. БланкаБланките на тези приложения са посочени в настоящите условия за DP.

1.Обхват

Настоящите условия на DP определят задълженията на обработващия лични данни към администратора на данни, свързани с предоставянето на услуги от обработващия данни съгласно споразумението.

Дейностите по обработване, целите на обработването, категориите лични данни, които ще бъдат обработвани, и категориите физически лица ще бъдат описани подробно в споразумението, като се използва приложение 1 към настоящите условия на DP

2. Продължителност

Разпоредбите на настоящите условия за DP се прилагат по време на срока на всяко съответно споразумение. Изтичането или прекратяването на споразумението не освобождава страните от съответните им задължения по отношение на поверителността на данните и защитата на личните данни, докато обработването се извършва след изтичане или прекратяване.

3. Интерпретация и йерархия

Позоваването в тези условия на DP на „писане“ или „писмено“ включва имейл.

Ако има противоречие между разпоредбите на настоящите Условия за DP и Споразумението, разпоредбите на настоящите Условия за DP имат предимство, доколкото конфликтът се отнася до Лични данни, освен ако страните по Споразумението изрично не се отклоняват от настоящите Условия за DP.

4.Определения

Всички термини с главни букви, използвани в настоящите условия за DP, имат значенията, определени в таблицата по-долу.

Термин	Определиние
Изисквания за защита на данните	Означава всички приложими закони и разпоредби, свързани с Обработка на лични данни, включително общите данни Регламент за защита (Регламент (ЕС) 2016/679) (“**GDPR**”),

Термин	Определиние
	специфични за сектора закони и приложими насоки и кодекси за практика, издадени от надзорни органи..
Лице	Означава идентифицирано или идентифицируемо физическо лице, за което се отнасят Личните данни. Подлежащо на идентификация физическо лице е това, което може да бъде идентифицирано, пряко или косвено, по-специално чрез позоваване на идентификатор като име, идентификационен номер, данни за местоположението, онлайн идентификатор или на един или повече фактори, специфични за физическите, физиологичните, генетичните ,психическа, икономическа, културна или социална идентичност на това физическо лице. То се отнася до служители и свързания с тях персонал, клиенти, бизнес партньори или други трети страни, чиито лични данни се обработват
Лични данни	Означава всякаква информация, свързана с физическо лице.

Обработка	Означава всяка операция или набор от операции, извършени върху Лични данни или върху набори от Лични данни, независимо дали чрез автоматизирани средства, като събиране, записване, организиране, структуриране, съхранение, адаптация или промяна, извличане, консултация, използване, разкриване чрез предаване , разпространение или предоставяне по друг начин, подравняване или комбинация, ограничаване, изтриване или унищожаване.
Нарушение на сигурността на личните данни	Нарушение на сигурността, водещо до случайно или незаконно унищожаване, загуба, изменение, компрометиране, неразрешено разкриване или достъп до лични данни, предавани, съхранявани или обработвани по друг начин от или от името на Allianz, и което поражда регулаторни задължения.
Оценка на Въздействието Върху Поверителността или PIA	Означава структуриран и повторяем анализ на инициативи и съществуващи или планирани промени, засягащи бизнес процеси, процедури, системи, продукти или услуги, включващи Обработката на лични данни. Този анализ предоставя информация за идентифициране, оценка и смекчаване на рисковете за поверителност и защита на данните и описва адекватни и пропорционални мерки за намаляване на въздействието и вероятността от рискове за поверителност и защита на данните, включително технически и организационни мерки (например регламенти, процедури, насоки, правни договори, управление практики или организационни структури).
TOMs	Означава оперативни, управленски, физически, технически и организационни мерки, както е посочено в раздел 9.1.

5.Инструкции

5.1 Обработващият данни обработва лични данни само (i) в рамките на настоящите условия на DP, (ii) Изискванията за защита на данните и (iii) по документирани инструкции от Администратора на данни, включително по

отношение на прехвърлянето на лични данни към трета държава или международна организация, освен ако това не се изисква от Изискванията за защита на данните, на които обработващият данни е обект; в такъв случай обработващият данни информира администратора на данни за това законово изискване преди обработката, освен ако изискванията за защита на данните не забраняват такава информация на важни основания от обществен интерес.

5.2 Обработващият лични данни посочва лице, което е надлежно квалифицирано за Изискванията за защита на данните, което е упълномощено да представлява обработващия данни по отношение на настоящите Условия за DP и да получава инструкции от Администратора на данни. Обработващият данни незабавно информира Администратора на данни в писмен вид, ако смята, че която и да е инструкция, издадена от Администратора на данни, нарушава Изискванията за защита на данните.

6.Предоставяне на информация и подкрепа

По искане на Администратора на данни, Обработващият лични данни предоставя цялата информация, необходима за спазване на Изискванията за защита на данните. Освен това обработващият данни подкрепя администратора на данни при изпълнението на изискванията за защита на данните, по-специално по отношение на неприкосновеността на личния живот чрез проектиране, записи на дейностите по обработка, сътрудничество или консултации с и уведомяване на компетентния надзорен орган, сигурност на обработката и провеждане на PIA.

7. Подобработващи

7.1 Изискване за одобрение

Обработващият данни няма да ангажира друг обработващ данни като негов под-обработващ без специално или общо писмено разрешение на Администратора на данни, което се посочва в Споразумението, с изключение на одобрените под-обработващи, изброени в Приложение 2 към настоящите условия за DP , които трябва да бъдат попълнени в Споразумението.

В случай на общо упълномощаване, обработващият данни информира администратора на данни за всички планирани промени, свързани с добавянето или подмяната на подизпълнители, като по този начин

предоставя на администратора на данни възможност да възрази срещу такива промени.

7.2 Ангажиране на подобработващи

Обработващият данни ще ангажира само под-обработващ (i), който предоставя достатъчни гаранции за прилагане на подходящи технически и организационни мерки по такъв начин, че обработването да отговаря на изискванията на настоящите Условия на DP и изискванията за защита на данните, и (ii) чрез влизане в правно обвързващо споразумение, което поставя същите задължения за защита на данните, включително задълженията за поверителност, или еквивалентен или по-висок стандарт като тези, определени в настоящите Условия за DP за под-обработващ, при условие че ако под-обработващият не изпълни задълженията си за защита на данните, обработващият данни остава изцяло отговорен пред администратора на данни за изпълнението на задълженията на под-обработващия.

7.3 Всяка по-нататъшна допълнителна обработка не е разрешена без предварителното конкретно или общо писмено съгласие на Администратора на данни и ще се извършва само в съответствие с гореспоменатите изисквания.

8. Без по-нататъшно прехвърляне на лични данни

Обработващият данни няма право да прехвърля лични данни на подизпълнител, разположен извън Европейското икономическо пространство, без предварителното писмено съгласие на Администратора на данни. В такъв случай на трансфер на данни извън Allianz Group, се разрешава само ако под-обработващият, който не е от ЕИП, сключи подходящи договорни споразумения с Администратора на данни, за да осигури адекватно ниво на поверителност и защита на данните по отношение на Лични Данни в такава форма, както е предписано от Изискванията за защита на данните и / или одобрено от приложимия надзорен орган. Такива договорни споразумения могат да включват, по указание на Администратора на данни, стандартните клаузи на ЕС за защита на данните за прехвърляне на лични данни към трети държави.

9. Поверителност

Обработващият лични данни трябва да спазва тайната на данните и да поддържа поверителност при обработката на лични данни съгласно настоящите Условия на DP и ще ги осигури от всеки персонал, ангажиран

във връзка с тези Условия за DP. Следователно обработващият данни ангажира служители за обработка на лични данни, които са правилно инструктирани, адекватно и редовно обучени относно изискванията за защита на данните, свързани с тяхната работа.

Когато личните данни подлежат на одити, инспекции, разследвания, издирване и изземване, запор за запор, конфискация по време на производство по несъстоятелност или несъстоятелност, заповед за разкриване, всяко (включително висящо или заплашено) изпълнително производство, иск, съдебен иск, заведен или заплашен срещу обработващия данни или под-обработващ, отнасящ се до Лични данни, или подобни събития или мерки от трети страни, Обработващият данни информира Администратора на данни за това без ненужно забавяне.

10. Изтриване или връщане на лични данни

При прекратяване или изтичане на споразумението, обработващият данни, по искане на Администратора на данни, изтрива или връща в структуриран, често използван и машинно четим формат всички съществуващи копия, документи, Обработка и резултати от работата и набори от данни, свързани с Условията за DP , освен ако приложимото законодателство изисква съхранение на такива Лични данни.

Обработващият лични данни потвърждава писмено, че е спазил настоящия раздел 10 и предоставя журнал на изтриването по искане на Администратора на данни.

11. Технически и организационни мерки; Записи

11.1 Технически и организационни мерки

За да осигури ниво на сигурност, подходящо за риска, обработващият данни, вземайки предвид състоянието на техниката, разходите за изпълнение и естеството, обхвата, контекста и целите на обработката, както и риска от промяна вероятност и тежест за правата и свободите на физическите лица и да прилага и поддържа оперативни, управленски, физически, технически и организационни мерки („TOM“) за защита на личните данни срещу случайно, неразрешено или незаконно унищожаване, загуба, изменение, разкриване или достъп подходящи за риска по отношение на поверителността, целостта, наличността и устойчивостта на системите, както се изисква от изискванията за защита на данните

TOMs на обработващия данни по всяко време осигуряват стриктно разделение между обработваните лични данни съгласно настоящите

условия на DP, собствените данни на обработващия данни и данните на другите клиенти на обработващия данни.

TOMs, внедрени от обработващия лични данни към датата на настоящите условия за DP, са посочени в приложение 3 към настоящите условия за DP, което трябва да бъде попълнено в споразумението.

11.2 Записи

Обработващият данни трябва да поддържа и поддържа точни писмени записи на всички дейности по обработка и промени в TOM в съответствие с изискванията за защита на данните.

12. Нарушения на личните данни

12.1 Задължение за уведомяване

Обработващият данни предоставя на администратора на данни подробно писмено известие (на вниманието на длъжностното лице по защита на данните на администратора на данни / специалист по поверителност на данните и, когато е уместно, на главния служител по сигурността на информацията) без ненужно забавяне, но не по-късно от двадесет и четири (24) часа: (i) за откриване или информиране за всяка загуба или неоторизиран достъп до лични данни, обработвани от Обработващ данни или под-обработващ; или (ii) всяко нарушение на Изискванията за защита на данните от страна на обработващия лични данни или под-обработващ („Нарушаване на личните данни“). Известието включва по-специално описание на: (i) естеството на нарушението на личните данни; (ii) вероятните последици от нарушаването на личните данни; и (iii) мерките, предприети или предложени да бъдат предприети за преодоляване на нарушенията на личните данни. В този случай обработващият данни, в допълнение към всяко задължение, съдържащо се в настоящите условия на DP и Споразумението, за своя сметка:

(a) да извърши съдебен преглед и одит на състоянието на техниката във връзка с нарушение на личните данни и да информира администратора на данни за резултата от този преглед и предприетите коригиращи и превантивни действия, за да се избегнат идентични или подобни нарушения на лични данни в бъдеще; и

б) разумно да си сътрудничи с Администратора на данни в отговор на такова нарушение на личните данни и предприемане на необходимите коригиращи и / или превантивни действия.

13. Коригиране, ограничаване и заличаване; Права на лицата

Allianz

Обработващият данни не може сам да коригира, изтрие или ограничи Обработката на лични данни, а само по писмените указания на Администратора на данни. Обработващият данни информира Администратора на данни незабавно, след като узнае за грешки или неточности, свързани с Лични данни, които могат да възникнат във връзка с Обработката. Обработващият данни незабавно коригира всички грешки или неточности в Личните данни при писмено искане на Администратора на данни.

В случай, че дадено физическо лице се свърже с обработващия лични данни директно по отношение на неговите Лични данни с искане за достъп, коригиране, изтриване, ограничаване или възражение срещу обработката на личните му данни или за автоматизирани решения, или преносимост на данни, обработващият данни незабавно препраща искането на физическото лице до администратора на данни.

Обработващият данни съдейства на Администратора на данни в отговор на искания от Лица, упражняващи гореспоменатите си права по отношение на техните Лични данни. Това включва по-специално следното: при поискване от администратора на данни, Обработващият (i) ще предостави без неоправдано забавяне на Администратора на данни копие от Личните данни на Физическото лице в структуриран, често използван и машинно четим формат или по преценка на Администратора на данни, ще осигури разумен достъп до Личните данни и (ii) незабавно предоставя на Администратора на данни информация относно обработката на лични данни, която Администраторът на данни може разумно да поиска

14. Одити

Обработващият данни разрешава на Администратора на данни, назначените от него одитори и при необходимост компетентните надзорни органи да инспектират и одитират операциите по обработка на Обработващия данни (включително по отношение на изпълнението на ТОМ) и спазването на инструкциите на Администратора на данни и Изискванията за защита на данните. Обработващият данни предоставя на одиторите (включително техните съответни упълномощени представители) цялата информация и права за достъп (включително до помещения и бази данни), свързани с Обработката на личните данни.

В случай на констатации, произтичащи от такива инспекции или одити, обработващият данните незабавно предприема всички необходими коригиращи действия за своя сметка.

Allianz

Обработващият данни одитира периодично (поне веднъж годишно) неговото съответствие и съответствието на неговите под-обработващи лица с настоящите Условия на DP и изисквания за защита на данните по отношение на обработката. Предишният параграф се прилага mutatis mutandis към констатациите при такива самоодити. Обработващият данни незабавно уведомява Администратора на данни в писмен вид за всички констатации, показващи, че обработващият данни или обработката на лични данни не отговаря на изискванията за защита на данните или на разпоредбите на настоящите условия на DP и / или споразумението и предоставят на Администратора на данни доклад, обобщаващ констатациите от одита.

Ако одитите се извършват от надзорен орган в Allianz Group, който изцяло или частично се отнася до настоящите Условия за DP, обработващият данни осигурява и гарантира, че неговите под-обработващи лица осигуряват подкрепа за Администратора на данни в рамките на настоящите условия на DP.

Ако надзорен орган, компетентен за Администратора на данни, извършва одит на Обработващия лични данни във връзка с Обработката, този одит се извършва в присъствието на Администратора на данни.

Ако надзорен орган, компетентен за обработващия данни, извърши одит при обработващия данни, обработващият данните незабавно уведомява администратора на данни, по-специално по отношение на всички констатации, които оказват пряк или косвен ефект върху договорните отношения.

Бланка ПРИЛОЖЕНИЕ 1 Дейности за описание и обработка на данни

Администратор на данни

Администраторът на данни е (моля, посочете):

_____

_____

Обработващ данни

Обработващ данни е (моля, посочете):

_____

_____

Цел на обработката

Ако вече не е посочено в споразумението, личните данни ще бъдат обработвани за следната цел:_____ (моля, посочете).

Продължителност на обработката

Allianz

Личните данни ще бъдат обработвани за срока на действие на споразумението.

Физически лица

Обработените лични данни се отнасят до следните категории физически лица

(моля, посочете):

- ☐ Служители
- ☐ Кандидати
- ☐ Физически лица на доставчика (включително агенти, посредници,…)
- ☐ Бизнес партньори (доставчици,клиенти, брокери,посредници…)
- ☐ Застраховани лица/Титуляри на договори
- ☐ Застраховани
- ☐ Бенефициенти
- ☐ Роднини на притежатели на договори (титуляри на полици, осигурени или бенефициенти)

Друго (моля посочете):

_____

Категории лични данни

Обработените лични данни се отнасят до следните категории лични данни (моля, изберете по подходящ начин и посочете допълнително в полетата за въвеждане по-долу, отбелязани със *)):

Основни лични данни

- ☐ Име / собствено,бащино и фамилия
- ☐ Възраст/дата на раждане
- ☐ Пол
- ☐ Адрес
- ☐ E-mail
- ☐ Телефонен номер

Други средства за контакт (моля посочете):

_____

Доказателство за самоличност (лична карта, паспорт,…)

Националност

Друго (моля посочете):

_____

Образователен професионален опит и принадлежности

☐ История на образованието и обучението

☐ Квалификация/сертификати

☐ Езици

☐ Информация за предишен работодател

☐ История на предишна работа

☐ Членство в синдикати*

Друго (моля посочете):

_____

Бизнес дейности

☐ Бизнес дейности на физическо лице

☐ Предоставени стоки или услуги

☐ Друго (моля посочете):

_____

Информация за пътуванията и разходите на служителите

☐ Подробности за резервации при пътуване

☐ Диетични изисквания

☐ Подробности относно искания за разходи

☐ Референции относно пътувания и изисквания за ваучери

☐ Подробности относно виза и паспорт

Друго (моля посочете):

_____

Семейство, начин на живот и социален статус

- ☐ Семейно положение
- ☐ Финансово зависими лица/съпруг/партньор/подробности за семейството
- ☐ Следваща информация/ контакти при спешни случаи
- ☐ Етническа принадлежност*
- ☐ Религия/религиозни вярвания*
- ☐ Друга информация относно многообразието и равенството* (моля посочете): _____

Основни данни за служителите/ HR данни

- ☐ Персонален номер
- ☐ Заемана длъжност/позиция
- ☐ Работен статус-пълно работно време / непълно работно време
- ☐ Данни относно кандидатурата за работа (напр.формуляр за кандидатсване, бележки от интервю, справки и др.)
- ☐ Детайли/описание на позицията
- ☐ Данни относно здравно осигуряване
- ☐ Образователна степен
- ☐ Фирма/юридическо лице
- ☐ Бизнес единица/подразделение
- ☐ Местоположение на офиса
- ☐ Линия/мениджър за докладване
- ☐ Начална дата
- ☐ Работни часове
- ☐ Дати и подробности за преместване
- ☐ Крайна дата и причини за прекратяване
- ☐ Вид договор (фиксирани условия/временен/постоянен)
- ☐ Друго (моля посочете):

_____

Здраве, благосъстояние и отсъствия

- ☐ Запис на отсъствие/проследяване на работно време/годишен отпуск*
- ☐ Причина за отсъствие*
- ☐ Детайли за физическото и психологическото здраве или медицинско състояние*
- ☐ Информация и докладване, свързани със здравето и безопасността*
- ☐ Информация и докладване, свързани със здравето на работното място*
- ☐ Неволи и оплаквания* ?
- ☐ Детайли свързани с притесняване и тормоз*

Детайли относно инвалидност,достъп, специални изисквания*

Пенсиониране по здравословни причини*

Друго (моля посочете):

_____

Свързани с представянето на служителите

- ☐ Дисциплинарни мерки
- ☐ Изходящи интервюта и коментари
- ☐ Отговори на анкети (напр.връзка с поведенчески данни)
- ☐ Прегледи за лично развитие (дата на прегледа, детайли и коментари)
- ☐ Рейтинг на ефективността

Други отзиви,коментари и анализи свързани с изпълнението (моля посочете):

_____

Финансови данни

- ☐ Информация за банкова сметка
- ☐ Информация за банкова карта
- ☐ Национален осигурителен номер
- ☐ Работна заплата
- ☐ Очаквани плащания/заплата
- ☐ Удръжки от трети страни
- ☐ Данъчен кодекс ?/Tax Code
- ☐ Бонус плащания
- ☐ Данни за компенсации
- ☐ Данни за права и обезщетения
- ☐ Данни относно членство в споделена схема
- Подпомагане за жилище и преместване

Друго (моля посочете):

_____

Информация относно фотографии,видеа и местоположение

- ☐ Фотографски и видео изображения, включително CCTV изображения
- ☐ Местоположение/данни за проследяване
- ☐ I.P. Адрес

Друго (моля, посочете):

_____

Проверки за идентификация и минало

- Резултати от наказателни проверки*
- Проверка свързана с кредит
- Препоръки и данни за препоръчващ

- ☐ Данни относно свидетелство за управление на МПС
- ☐ Доказателство относно допустимост за работа (напр.данни от виза, паспорт)
- ☐ Данни от лична карта
- ☐ Подпис
- ☐ Банкови извлечения
- ☐ Обединени сметки
- ☐ Удостоверение за раждане
- ☐ Външни директорски постове и външни бизнес интереси
- ☐ Детайли за получени подаръци,покани за събития и друг вид гостоприемство

Друго (моля,посочете):

_____

Специални категории лични данни (ако е уместно)

Обработените лични данни се отнасят до следните специални категории данни (моля, изберете според случая):

- ☐ Расов или етнически произход
- ☐ Политически мнения
- ☐ Религиозни вярвания
- ☐ Философски вярвания
- ☐ Членство в Синдикати
- ☐ Генетични данни
- ☐ Биометрични данни
- ☐ Здраве
- ☐ Сексуален живот
- ☐ Сексуална ориентация
- ☐ Наказателни присъди и престъпления

Процеси по обработка

Личните данни ще бъдат предмет на следните основни дейности по обработване (моля, посочете):

- ☐ Събиране
- ☐ Записване
- ☐ Структуриране
- ☐ Съхраняване
- ☐ Адаптиране или промяна
- ☐ Извличане
- ☐ Консултация
- ☐ Използване
- ☐ Разкриване чрез предаване
- ☐ Разпространение или предоставяне по друг начин
- ☐ Подравняване или комбиниране
- ☐ Ограничение
- ☐ Изтриване или унищожаване

Други начини свързани с процесите по обработка (напр.Комуникация, …)

Бланка ПРИЛОЖЕНИЕ 2 Одобрени подобработващи

Следните компании с настоящото са предварително упълномощени да извършват работа като под-обработващи на обработващия данни: (моля, предоставете информацията по-долу за всеки под-обработващ, обхванат от това разрешение

Корпоративно име на подобработващия
Регистрирани офиси на подобработващия
Помещения, в които подобработващия, ще извърши обработка
Цел на обработката, извършена от подобработващия
Дейности свързани с обработването
Продължителност на обработката
Категории физически лица
Категории лични данни
Категории на специални категории лични данни
Представител на подобработващия, отговорен за поверителността на данните (напр. Длъжностно лице по защита на данните) и данни за контакт

Бланка ПРИЛОЖЕНИЕ 3

Технически и организационни мерки за сигурност

_____

_____

_____

_____

Приложение D : Обработка на молби и жалби на физически лица, свързани с данни за ЕИП [33]

Процедурата, посочена в настоящото приложение D , се прилага за Данни от ЕИП по отношение на искания и жалби от физически лица съгласно глава D , раздели I. до V. и жалби на Физически лица за нарушения на изискванията за BCR трансфери съгласно глава C,Раздел III.

Администраторите на данни за ОЕ трябва да се придържат към процедурата, описана по-долу, за да улеснят упражняването на правото на физическо лице на:

- Достъп, коригиране, изтриване, възражение, ограничение, преносимост и правата, свързани с автоматизирани индивидуални решения (включително профилиране);

- Оплакване по всеки въпрос, свързан с Изискванията за обработка в ЕИП, съгласно който се обработват неговите лични данни; и

- Оплакване се за всяко нарушение на Изискванията за прехвърляне на BCR, при което неговите лични данни се прехвърлят към ОЕ извън ЕИП.

Специалистът по поверителност или DPP / DPO на администратора на данни на ОЕ при произхода на обработката, според случая, е отговорен за обработката на такива искания и жалби.

I. Потвърждение на самоличността на физическо лице

Когато е приложимо, специалиста по поверителност (Privacy Champion) или DPP / DPO, действащ от името на администратора на данни на ОЕ, според случая, има някакво основателно съмнение относно самоличността на физическо лице, което прави искането или жалбата, или когато това се изисква от приложимите закони и разпоредби на ЕИП, той / тя може да поиска допълнителни информация, за да се потвърди самоличността на Физическото лице, освен ако искането или жалбата са свързани с автоматизирани решения (включително Профилиране).

II. Процес и срокове за обработка на искания и жалби

Следващите стъпки очертават процеса, който трябва да се предприеме от Специалиста по поверителност или DPP / DPO на OE Data Controller при обработка на искания и жалби на физически лица:

Стъпка 1:

Да потвърди получаването на оплакването от лицето в рамките на две седмици от получаването и да го информира относно процедурата и сроковете за отговор.

Стъпка 2

Проучва обстоятелствата свързани с предмета на оплакването, и събира необходимата за отговора информация.

Стъпка 3

Предоставя на лицето информация за всяко действие, предприето в допълнение към неговото / нейното оплакване, без ненужно забавяне и във всеки случай не по-късно от един месец от получаването на оплакването.

Ако в хода на разследването се установи, че едномесечният срок за отговор не може да бъде спазен, като се вземе предвид сложността и обхвата на жалбата и, определения Специалист по поверителност, в сътрудничество с OE DPP / DPO , информира Физическото лице за всяко удължаване в рамките на един месец от получаването на искането, заедно с причините за забавянето и очаквания график за разглеждане на искането или жалбата (този период не трябва да бъде по-дълъг от два месеца, с изключение на извънредни обстоятелства). Когато е уместно, OE Champion или DPP / DPO може да се свърже с GCPO, за да обработи сложна молба или жалба.

Стъпка 4

Ако разследването разкрие, че оплакването е оправдано, си сътрудничи с Управителния съвет на OE Data Controller и, определения Специалист по поверителност, си сътрудничи със съответния DPP / DPO, както и с GCPO, според случая, за прилагане на съответни мерки за адресиране на искането или разрешаване на жалбата, информиране на лицето за констатациите и съответните мерки за отстраняване, както и правото на лицето да ескалира оплакването до

GCPO, ако той / тя е недоволен от резултата или обработката на неговото / нейното оплакване.

Ако разследването разкрие, че оплакването не е оправдано, информира лицето без ненужно забавяне и във всеки случай, не по-късно от един месец, за (i) констатациите заедно с мотиви, (ii) правото да отправи оплакване до GCPO, ако той / тя желае да оспори отговора, когато оплакването на лицето е отхвърлено, и (iii) правото на лицето да подаде жалба до компетентен орган за защита на данните в ЕИП и да потърси съдебни средства за защита.

Когато на Специалиста по поверителност е възложено от DPP / DPO да обработва искания и жалби, Специалиста по поверителност трябва да информира DPP / DPO за всички предприети стъпки и за научената информация

III. Контакт и форма на отговор на физическо лице

Администраторите на данни за ОЕ трябва да предоставят на лицата данните за контакт на ОЕ DPO / DPP в известия за поверителност, за да улеснят упражняването на тези права.

За жалби относно BCRs трансфери, ОЕ администраторите на данни трябва да насочат физическите лица да подадат своите жалби, като изпратят имейл на privacy@allianz.com.

Когато лице отправя искане по електронен път, администраторът на данни за ОЕ трябва да предостави всякаква информация по електронен път в често използвана електронна форма, когато е възможно, освен ако лицето не изисква друго. Ако информацията, предоставена на лицето, включва лични данни или поверителна информация, администраторът на данни за ОЕ трябва да осигури подходящи предпазни мерки, когато ги предоставя лицето, така че да осигури тяхното безопасно предаване (например чрез криптиране).

IV. Разходи

Всяко съобщение и всяко действие, предприето от администратора на данни на ОЕ в отговор на упражняването на правата или жалбата на дадено лице, трябва да се предоставят безплатно, с изключение на това, че може да бъде начислена разумна такса, ако:

- Заявките са явно неоснователни или прекомерни, по-специално поради техния повтарящ се характер, като в този случай

администраторът на данни за ОЕ носи тежестта да демонстрира явно необоснован или прекомерен характер на исканията или жалбите; или
- Изискват се допълнителни копия на лични данни

V. Отказ за предприемане на действия по искане или жалба на физическо лице

Администраторите на данни за ОЕ могат да откажат да предприемат действия по искания или оплаквания, когато:

- Те са явно необосновани или прекомерни, по-специално поради техния повтарящ се характер, а ОЕ Data Controller може да демонстрира явно необоснован или прекомерен характер на исканията или жалбите;
- Обработката не изисква идентификация и Администратора на данни за ОЕ може да докаже, че не е в състояние да идентифицира лицето; или
- Правото на лицето е изрично ограничено от приложимите закони и разпоредби на ЕИП

В случай на заявки за заличаване на лични данни, администраторите на данни за ОЕ също могат да откажат да предприемат действия, ако е необходима обработката:

- Да упражняват правото на свобода на изразяване и информация;
- Да спазва законите и разпоредбите на ЕИП, на които е подчинен администраторът на данни за ОЕ, които изискват обработка, или за изпълнението на задача, извършена в обществен интерес или при упражняването на официална власт, поверена на администратора на данни за ОЕ; или
- За установяване, упражняване или защита на правни искове.

VI. Известие до получателите

Когато заявката се отнася до правата за коригиране или заличаване на лични данни или за ограничаване на обработването, администраторите на ОЕ данни трябва:

- Да съобщават за коригиране или изтриване на лични данни или ограничаване на обработването на всеки получател, на когото личните данни са разкрити, освен ако това се окаже невъзможно или включва непропорционални усилия; и
- По искане на физическо лице да информира физическото лице за тези получатели.

Приложение E: Преглед на изискванията за APS

		Минимални изисквания на Глобално ниво	Изисквания за обработка в ЕИП	Изисквания за трансфери съгласно BCRs
A.	**Представяне**			
I.	Обосновка	1	2	1
II.	Одобрение и актуализация	1	2	1

B.	**Принципи за спазване на изискванията за поверителност защитата на данните**			
I.	Дължима грижа	1	2	1
II.	Качество на данните			
1.	Ограничение на целта			
1.1.	*Минимални изисквания на Глобално ниво*	1	2	3
1.2.	Допълнителни изисквания за обработка в ЕИП и трансфери на BCR		2	3
2.	Минимизиране и точност на данните	1	2	3
3.	Ограничение на съхранението	1	2	1
III.	Прозрачност и откритост			
1.	Минимални изисквания на Глобално ниво	1	2	1
2.	Допълнителни изисквания за обработка в ЕИП трансфери съгласно BCR			
2.1.	Информация, събрана от физическото лице		2	1
2.2.	Информация, събрана от други източници		2	1
IV.	Законозъобразност на обработването			
1.	Минимални изисквания на Глобално ниво	1	2	3

2.	Условия за съгласие при обработка в ЕИП и трансфери съгладноBCRs		2	3
3.	Законосъобразност при обработване на Чуствителни лични данни в ЕИП и трансфери съгладноBCRs		2	3
4.	Законосъобразност на обработването за наказателни присъди и престъпления за обработка в ЕИП и трансфери съгладноBCRs		2	1
V.	Връзка с обработващите данни			
1.	Минимални изисквания на Глобално ниво	1	2	1
2.	Допълнителни изисквания за обработка в ЕИП трансфери съгласно BCR		2	1
VI.	Трансфери и последващи трансфери			
1.	Минимални изисквания на Глобално ниво	1	2	1
2.	Допълнителни изисквания за обработка в ЕИП трансфери съгласно BCR		2	3
VII.	Сигурност и поверителност			
1.	Минимални изисквания на Глобално ниво	1	2	3
2.	Допълнителни изисквания за обработка в ЕИП трансфери съгласно BCR		2	3
VIII.	Инциденти или нарушения на лични данни			
1.	Минимални изисквания на Глобално ниво	1	2	1

2.	Допълнителни изисквания за обработка в ЕИП трансфери съгласно BCR		2	1

2.1.	Нотификация до компетентния орган за защита на данните в ЕИП		2	1
2.2.	Комуникация с физически лица		2	1
2.3.	Известие до администратора на данни		2	1
IX.	Поверителност по смисъл и по подразбиране			
1.	Поверителност по смисъл			
1.1.	Минимални изисквания на Глобално ниво	1	2	3
1.2.	Допълнителни изисквания за обработка в ЕИП трансфери съгласно BCR		2	3
2.	Поверителност по подразбиране за обработка в ЕИП и BCR трансфери		2	3
X.	Сътрудничество с органите за защита на данните в ЕИП за обработка на ЕИП и прехвърляне на BCR		2	1

C.	**Дейности и процеси за спазване на поверителността и защитата на данните**			
I.	Оценки на въздействието и етиката върху поверителността и записи на дейностите по обработка	1	2	1
II.	Обучение			
1.	Минимални изисквания на Глобално ниво	1	2	1
2.	Допълнителни изисквания за обработка в ЕИП трансфери съгласно BCR			1
III.	Механизъм за вътрешни оплаквания и жалби			
1.	Минимални изисквания на Глобално ниво	1	2	3
2.	Допълнителни изисквания за обработка в ЕИП трансфери съгласно BCR		2	3

IV.	Мониторинг и осигуряване			
1.	Минимални изисквания на Глобално ниво	1	2	3
2.	Допълнителни изисквания за обработка в ЕИП трансфери съгласно BCR			1

D.	**Задължения към физически лица**			
I.	Отговаряне на исканията на физически лица за достъп, коригиране или изтриване			
1.	Минимални изисквания на Глобално ниво	1	2	1
2.	Допълнителни изискванияза обработка в ЕИП трансфери съгласно BCR		2	1
2.1.	Искане за достъп		2	1
2.2.	Искане за коригиране		2	1
2.3.	Искане за изтриване		2	3
II.	Отговаряне на молбите на физически лица за възражение срещу обработване в ЕИП и трансфери на BCR		2	3
III.	Отговаряне на молбите на физически лица за ограничаване на обработването в ЕИП и трансфери съгласно BCR		2	3
IV.	Отговаряне на исканията на физически лица за преносимост за обработка в ЕИП и трансфери съгласно BCR		2	1
V.	Отговаряне на исканията на физически лица за възражение срещу автоматизирани решения за обработка в ЕИП и трансфери съгласно BCR		2	1

E.	**Роли и отговорности**			
I.	На ниво Allianz Group			
1.	Управителният съвет на Allianz SE	1	2	1
2.	Group Privacy	1	2	1
3.	Group Chief Privacy Officer / Главен директор на групата за поверителност	1	2	3
II.	Регионално ниво и глобални линии на Allianz	1	2	3
III.	На ниво Allianz OE			
1.	OE Управителен съвет			
1.1.	*Global Responsibilities*	1	2	1
1.2.	Допълнителни изисквания за обработка в ЕИП трансфери съгласно BCR		2	1
2.	OE Data Privacy ı Officer Professional/Data Protectio			
2.1.	*Отговорности на Глобално ниво*	1	2	1
2.2.	Допълнителни изисквания за обработка в ЕИП трансфери съгласно BCR		2	1
3.	OE Специалист по поверителност			
3.1.	*Отговорности на Глобално ниво*	1	2	3
3.2.	Допълнителни изисквания за обработка в ЕИП трансфери съгласно BCR		2	3
4.	OE Собственик на информацията	1	2	3
IV.	Allianz Group and OE Steering	1	2	1
1.	Общност за поверителност и защита на данните на Allianz	1	2	1
2.	Консултативна група за поверителност на Allianz	1	2	1

F.	**Препратки**	1	2	3

Приложение A	Терминологичен речник	1	2	3
Приложение B	Трансфери съгласно BCR, покрити от APS			3
Приложение C	Минимални изисквания за договорните отношения между Администратор на данни и Обработващ данни за обработка в ЕИП и прехвърляне на BCR		2	1
Приложение D	Обработка на молби и жалби на физически лица, свързани с данни за ЕИП		2	1

Изменения и корекции

Версия	Дата	Причина и обяснение на промяната	Автори
2.0	10.04.2018	Приемане на ОКП (BCRs) от Алианц Груп. Този документ замества и заменя Стандарта на Алианц за поверителност на данните от 01.10.2013 г.	Philipp Räther, Kully Thandi
2.1	[●]	Изменения на Стандарта за поверителност на Allianz, за да се приведе в съответствие с Общия регламент за защита на данните на ЕС и референцията на работната група по член 29 относно BCR (WP256) rev. 01 приета на 6 февруари 2018 г.	Philipp Räther, Kully Thandi, Jason Glass
3.0	30.11.2020	Годишен преглед, включващ малки промени, включително добавянето на Функционалното правило за управление, наблюдение и осигуряване на поверителност в Рамката.	Philipp Räther, Jason Glass, Kathleen Ugalde