

# Обязательные корпоративные правила (ОКП)

## Статус: Окончательный вариант

Область применения:

Компания Fresenius SE & Co. KGaA и все ее аффилированные лица в соответствии с разделом 15 и далее Закона Германии об акционерных обществах, за исключением тех, которые относятся к бизнес-сегментам Fresenius Kabi, Fresenius Medical Care, Fresenius Helios и Fresenius Vamed.

Компания Fresenius Kabi Aktiengesellschaft и все ее аффилированные лица в соответствии с разделом 15 и далее Закона Германии об акционерных обществах, которые относятся к бизнес-сегменту Fresenius Kabi.



**Оглавление**

1	Определения .....	4
2	Цель.....	6
3	Объем .....	6
3.1	Территориальный охват.....	6
3.2	Охват данных и круг лиц .....	7
3.3	Связь между ОКП и Применимым законодательством о защите данных .....	7
3.4	Несоответствия норм Применимого законодательства и ОКП .....	8
4	Обязательный характер ОКП / Права сторонних бенефициаров.....	8
5	Организация по защите данных .....	9
6	Принципы защиты Персональных данных по ОКП.....	10
6.1	Законность .....	10
6.2	Прозрачность и справедливость .....	12
6.2.1	Обязательная информация .....	12
6.2.2	Дополнительная информация, которая должна быть предоставлена ..	13
6.2.3	Дополнительная информация, которая должна быть предоставлена в том случае, если данные получены от третьей стороны. ....	13
6.3	Ограничение целей .....	13
6.4	Минимизация данных .....	14
6.5	Точность.....	14
6.6	Ограничение хранения .....	14
6.7	Безопасность, целостность и конфиденциальность .....	14
6.7.1	Технические и организационные меры безопасности.....	14
6.7.2	Уведомление о нарушениях мер защиты в отношении Персональных данных .....	15
6.8	Подотчетность .....	15
6.8.1	Привлечение Обработчиков .....	16
6.8.2	(Последующие) Передачи Персональных данных .....	16
7	Оценка рисков в защите данных .....	17
8	Оценка воздействия на защиту данных.....	19
9	Права Физических лиц.....	19
9.1	Право на доступ к Персональным данным .....	19
9.2	Право на исправление Персональных данных .....	19
9.3	Право на удаление Персональных данных .....	20

9.4	Право на ограничение Обработки Персональных данных .....	20
9.5	Право на получение Персональных данных в портативном формате и на передачу Персональных данных .....	20
9.6	Право возражения против обработки персональных данных .....	20
9.7	Право не подвергаться автоматическому принятию решений .....	20
10	Соблюдение ОКП.....	21
10.1	Доступ к ОКП.....	21
10.2	Обработка претензий в отношении ОКП.....	21
10.3	Ответственность и правоприменение .....	22
10.4	Сотрудничество с надзорными органами .....	23
10.5	Обучение.....	23
10.6	Контроль .....	23
10.7	Обновление ОКП.....	24
11	Управление выходом .....	25
12	Список использованных источников .....	25
13	История изменений документа .....	25
	Приложение 1: Список сторон, связанных обязательствами по ОКП .....	25
	Приложение 2: Характер передаваемых Персональных данных.....	30

## 1 Определения

В настоящих ОКП термины, написанные с заглавной буквы, имеют следующие значения:

- i. **«Применимое законодательство о защите данных»** означает действующие законы о защите данных в юрисдикции, которые применимы к Стороне;
- ii. **«Применимое законодательство»** означает совокупность действующих и применимых к Стороне законов юрисдикции, за исключением Применимого законодательства о защите данных;
- iii. **«ОКП»** означает настоящий документ и все приложения к нему;
- iv. **«Контролер»** означает физическое или юридическое лицо, государственный орган, агентство или другой орган, который самостоятельно или совместно с другими определяет цели и средства обработки персональных данных;
- v. **«Консультант по защите данных»** или **«КЗД»** означает консультанта по защите данных, назначенного в рамках группы Fresenius на центральном уровне.
- vi. **«Оценка воздействия на защиту данных»** или **«ОВЗД»** означает определенную оценку рисков для выявления и оценки рисков нарушения конфиденциальности в процессе деятельности по обработке данных, которые могут привести к высоким рискам для прав и свобод физических лиц, с целью снижения этих высоких рисков.
- vii. **«Уполномоченный по защите данных»** или **«УЗД»** означает уполномоченного по защите данных, назначенного в рамках группы Fresenius в соответствии со статьей 37 Общего регламента ЕС по защите персональных данных (ОРЗД), который не должен получать никаких инструкций в отношении выполнения своих задач.
- viii. **«Организация по защите данных»** означает организацию по защите данных каждой Стороны, состоящую из (Местных) консультантов по защите данных и (если требуется по закону) соответствующего Уполномоченного по защите данных;
- ix. **«ЕЭЗ»** означает Европейскую экономическую зону;
- x. **«Сотрудник(и)»** означает любого представителя руководства или лицо, находящееся в трудовых или квазитрудовых отношениях со Стороной, в том числе сотрудников, временных работников, учеников, стажеров, интернов, а также консультантов и любых других лиц, интегрированных в операционные процессы соответствующей Стороны;
- xi. **«ЕС»** означает Европейский Союз;
- xii. **«Рамочный договор»** означает договор между Сторонами о присоединении к ОКП.
- xiii. **«Группа Fresenius»** для целей настоящих ОКП означает Fresenius SE & Co. KGaA (**«FSE»**) и всех ее аффилированных лиц в соответствии с разделом 15 и далее Закона Германии об акционерных обществах (**«Хозяйственное подразделение Fresenius»**), за исключением тех, которые относятся к бизнес-сегментам Fresenius Kabi, Fresenius Medical Care, Fresenius Helios и Fresenius Vamed; а также Fresenius Kabi Aktiengesellschaft (**«FK AG»**) и всех ее аффилированных лиц в соответствии с разделом 15 и далее Закона Германии об акционерных обществах, которые относятся к бизнес-сегменту Fresenius Kabi;
- xiv. **«Дальнейшая обработка»** означает обработку персональных данных Стороной, находящейся за пределами ЕС/ЕЭЗ, куда Персональные данные были первоначально переданы Стороной, связанной обязательствами по ОРЗД;
- xv. **«ОРЗД»** означает Регламент (ЕС) 2016/679 Европейского парламента и Совета от 27 апреля 2016 г. о защите физических лиц в отношении обработки персональных данных и о свободном перемещении таких данных, а также об отмене Директивы 95/46/ЕС;

- xvi. **«Физическое лицо/Физические лица»** означает идентифицированное или идентифицируемое физическое лицо; идентифицируемое физическое лицо — это лицо, которое можно идентифицировать прямо или косвенно, в частности, посредством ссылки на идентификатор, такой как имя, идентификационный номер, данные о местоположении, онлайн-идентификатор или на один или несколько факторов, специфичных для физической, физиологической, генетической, психической, экономической, культурной или социальной идентичности этого физического лица;
- xvii. **«Местный консультант по защите данных»** или **«МКЗД»** означает местного консультанта по защите данных, назначенного в рамках группы Fresenius на местном уровне.
- xviii. **«Последующая передача»** означает передачу персональных данных Стороной, находящейся за пределами ЕС/ЕЭЗ, другому получателю, находящемуся за пределами ЕС/ЕЭЗ, если Персональные данные изначально были переданы Стороной, связанной ОРЗД;
- xix. **«Сторона»** или **«Стороны»** означают хозяйственные подразделения группы Fresenius, связанные обязательствами по ОКП и указанные в Приложении 1;
- xx. **«Персональные данные»** означают любую информацию, относящуюся к идентифицированному или идентифицируемому физическому лицу («субъект данных»); идентифицируемое физическое лицо — это лицо, которое можно идентифицировать прямо или косвенно, в частности, посредством ссылки на идентификатор, такой как имя, идентификационный номер, данные о местоположении, онлайн-идентификатор или на один или несколько факторов, специфичных для физической, физиологической, генетической, психической, экономической, культурной или социальной идентичности этого физического лица;
- xxi. **«Обработка»** означает любую операцию или набор операций, которые выполняются с персональными данными или наборами персональных данных, как с использованием автоматизированных средств, такие как сбор, запись, организация, структурирование, хранение, адаптация или изменение, извлечение, консультирование, использование, раскрытие путем передачи, распространение или иное предоставление доступа, объединение или сочетание, ограничение, стирание или уничтожение, так и без их использования;
- xxii. **«Обработчик»** означает внутреннее или внешнее физическое или юридическое лицо, государственный орган, агентство или другой орган, который обрабатывает персональные данные от имени контролера;
- xxiii. **«Особые категории Персональных данных»** означают Персональные данные, раскрывающие расовое или этническое происхождение, политические взгляды, религиозные или философские убеждения или членство в профсоюзе, а также обработку генетической информации, биометрической информации с целью однозначной идентификации Физического лица, информацию, касающуюся здоровья, или информацию, касающуюся сексуальной жизни или сексуальной ориентации Физического лица;
- xxiv. **«Надзорный орган»** означает независимый государственный орган, учрежденный государством-членом ЕС в соответствии со статьей 51 ОРЗД;
- xxv. **«Соответствующий надзорный орган»** означает Надзорный орган, к ведению которого относится обработка персональных данных Стороной, поскольку:
- соответствующая Сторона учреждена на территории государства-члена этого надзорного органа;
  - соответствующая Сторона имеет свое основное или единственное предприятие на территории государств-членов того надзорного органа, откуда были переданы данные;

- Обработка существенно затрагивает или может существенно затрагивать Физических лиц, проживающих в государстве-члене
- xxvi. «**Сторонний получатель**» означает получателя Персональных данных, не являющегося Стороной ОКП;
- xxvii. «**Передача**» означает любую передачу Персональных данных от Контролера другому Контролеру, Обработчику или любому другому получателю.

В отношении терминов, не определенных в настоящем разделе, применяется документ Определение ОКП №16 и определения согласно ОРЗД.

## 2 Цель

Группа Fresenius работает по всему миру, включая те страны, в которых были приняты законы о защите данных и те, где не были приняты. В целях последовательного регулирования способа обращения с Персональными данными или их обработки, а также в целях соблюдения Группой Fresenius Применимого законодательства о защите данных, Стороны-участники ОКП соблюдают внутренний набор ОКП по Обработке Персональных данных, чтобы создать единообразный порядок обработки Персональных данных и адекватный уровень защиты данных во всех участвующих Сторонах по всему миру. Суть ОКП заключается в гармонизации стандарта защиты данных внутри Группы Fresenius на уровне защиты данных в соответствии со стандартами ЕС. Это обеспечивает обмен Персональными данными между всеми Сторонами с адекватным уровнем защиты данных по всему миру.

Одной из основных заинтересованных сторон в обеспечении надлежащего уровня защиты данных является группа Сотрудников, обрабатывающих Персональные данные в соответствующем хозяйственном подразделении Fresenius. Только в том случае, если эти Сотрудники знают о том, как следует обрабатывать Персональные данные и какие ограничения применяются, может быть достигнут адекватный стандарт защиты данных.

Эти ОКП содержат основные защитные меры и определяют их объем, цели, принципы и структуру.

## 3 Объем

### 3.1 Территориальный охват

- i. ОКП **применяются** в следующих сценариях:
  - Любая обработка Персональных данных Сторонами, расположенными в ЕС/ЕЭЗ (включая передачу другим Сторонам, независимо от того, находятся ли получатели в ЕС/ЕЭЗ или за их пределами);<sup>1</sup>
  - Любая обработка Персональных данных Сторонами, расположенными за пределами ЕС/ЕЭЗ, если такая обработка осуществляется «в контексте деятельности предприятия» Группы Fresenius в ЕС/ЕЭЗ (включая передачу другим сторонам независимо от того, находятся ли получатели на территории ЕС/ЕЭЗ или за ее пределами);<sup>1</sup>
  - Любая обработка Персональных данных Физических лиц, проживающих в ЕС/ЕЭЗ, Сторонами, расположенными за пределами ЕС/ЕЭЗ, если такая Обработка связана с (i) предложением товаров или услуг Физическим лицам в ЕС/ЕЭЗ, независимо от того, требуется ли оплата Физического лица, или (ii) мониторингом его поведения в

---

<sup>1</sup> Ст. 3 п. 1 ОРЗД

пределах ЕС/ЕЭЗ (включая Передачи другим Сторонам, независимо от того, находятся ли получатели в ЕС/ЕЭЗ или за их пределами);<sup>2</sup>

- Любая дальнейшая обработка Персональных данных Сторонами, расположенными за пределами ЕС/ЕЭЗ, в тех случаях, когда соответствующие Персональные данные были первоначально переданы Стороной, связанной обязательствами по ОРЗД;
  - Любая последующая передача Персональных данных Сторонами, расположенными за пределами ЕС/ЕЭЗ, другому получателю, находящемуся за пределами ЕС/ЕЭЗ, в тех случаях, когда соответствующие Персональные данные были первоначально переданы Стороной, связанной обязательствами по ОРЗД.
- ii. ОКП **не распространяются** на любую Обработку Персональных данных Сторонами, расположенными за пределами ЕС/ЕЭЗ, если такая обработка
- не осуществляется «в контексте деятельности учреждения» Группы Fresenius в ЕС/ЕЭЗ<sup>1</sup>
  - не связана с (i) предложением товаров или услуг Физическим лицам в ЕС/ЕЭЗ независимо от того, требуется ли оплата Физического лица, или (ii) мониторингом их поведения в пределах ЕС/ЕЭЗ,
  - не касается Персональных данных, которые были первоначально переданы Стороной, связанной обязательствами по ОРЗД.

### 3.2 Охват данных и круг лиц

- i. ОКП применяются к Обработке Персональных данных полностью или частично с помощью автоматизированных средств, а также к неавтоматизированной Обработке Персональных данных, которые являются частью файловой системы или предназначены для формирования части файловой системы.<sup>3</sup>
- ii. ОКП также применяются к тем Сторонам, которые Обрабатывают Персональные данные в качестве (внутреннего) Обработчика от имени другого хозяйственного подразделения Fresenius; однако лишь в том объеме, который не ведет к противоречию соответственно заключенного договора.
- iii. Во избежание сомнений, Персональные данные могут<sup>4</sup> передаваться только на основании ОКП между Сторонами, которые должным образом внедрили ОКП и подтвердили, что они успешно приняли меры по обеспечению соответствия ОКП.
- iv. ОКП применяются к Обработке Персональных данных каждой Стороной, указанной в Приложении 1 — Список сторон, связанных обязательствами по ОКП.
- v. ОКП в целом охватывают операции по Обработке, указанные в Приложении 2 «Характер передаваемых Персональных данных».

### 3.3 Связь между ОКП и Применимым законодательством о защите данных

Каждая Сторона будет придерживаться настоящих ОКП и соблюдать их, несмотря на то, что Применимое законодательство о защите данных может предусматривать другой или более низкий уровень защиты. Однако, если и в той степени насколько Применимое законодательство о защите данных предусматривает более строгие правила Обработки,

---

<sup>2</sup> Ст. 3 п. 2 ОРЗД

<sup>3</sup> Ст. 3 п. 1 ОРЗД

<sup>4</sup> Ст. 46 п. 2 (Б) и ст. 47 ОРЗД



Стороны в дополнение к ОКП будут соблюдать эти более строгие правила в соответствии с Применимым законодательством о защите данных.

### **3.4 Несоответствия норм Применимого законодательства и ОКП**

Каждая Сторона, связанная ОРЗД, в ходе оценки рисков в соответствии с разделом 7 перед первоначальной Передачей Персональных данных другой Стороне, находящейся за пределами ЕС/ЕЭЗ, должна оценить, способна ли последняя соблюдать на практике гарантии, предусмотренные ОКП.

Если у Стороны есть основания полагать, что Применимое законодательство или Применимое законодательство о защите данных препятствует соблюдению ОКП соответствующей или другой Стороной, или если это событие может оказать существенное влияние на стандарты, предусмотренные ОКП, соответствующая Сторона должна немедленно проинформировать об этом соответствующего Уполномоченного по защите данных, чтобы оценить влияние и разрешить конфликт, последний, в свою очередь, должен проинформировать штаб-квартиру ЕЭЗ или организацию ЕЭЗ, на которую возложены соответствующие обязанности.

Если юридическое требование, такое как обязательное распоряжение о раскрытии Персональных данных, применимое к Стороне, оказывает существенное неблагоприятное воздействие на гарантии, которые Группа Fresenius установила посредством ОКП, соответствующая Сторона должна сообщить об этой проблеме, указав запрашиваемые данные, наименование запрашивающего органа, а также правовые основания соответствующему Местному консультанту по защите данных, который должен проинформировать соответствующего Уполномоченного по защите данных, который, в свою очередь, должен проинформировать штаб-квартиру ЕЭЗ или организацию ЕЭЗ, на которую возложены соответствующие обязанности. Надзорный орган в Гессене, Германия, будет проинформирован соответствующим Уполномоченным по защите данных. Вся информация должна предоставляться оперативно.

В случае если такое уведомление запрещено Применимым законодательством, Сторона приложит все усилия для получения разрешения на информирование соответствующего Уполномоченного по защите данных, а затем и Надзорного органа в Гессене, Германия, как можно скорее, предоставив информацию в максимально возможном объеме.

Если Стороне не разрешено предоставлять конкретную информацию по запросу, Сторона будет предоставлять общую информацию о запросах соответствующему Уполномоченному по защите данных, получаемых на ежегодной основе, с предоставлением соответствующей информации в максимально допустимом объеме (в частности, указывая количество полученных и исполненных приказов о раскрытии информации, запрашивающие органы, затронутые категории Физических лиц и виды Персональных данных) для того, чтобы была возможность проинформировать Надзорный орган в Гессене, Германия.

В любом случае Передача Персональных данных Стороной любому органу государственной власти не может быть массовой, непропорциональной и неизбирательной, выходящей за рамки того, что является необходимым в демократическом обществе.

## **4 Обязательный характер ОКП / Права сторонних бенефициаров**

ОКП являются обязательными для каждой Стороны и ее Сотрудников. Физические лица являются сторонними бенефициарами и могут получать права по ОКП. Каждая Сторона и каждый из ее Сотрудников обязаны уважать принципы и обязательства, изложенные в ОКП.

Обязательный характер ОКП включает в себя:

- i. *Обязательный характер для Сторон.* Группа Fresenius внедрила ОКП среди Сторон и создала механизм, чтобы сделать ОКП обязательными для любой Стороны, указанной в Приложении 1 «Список Сторон, связанных обязательствами по ОКП». Подписав Рамочный договор со всеми участвующими Сторонами, каждое хозяйственное



подразделение Fresenius взяло на себя договорные обязательства соблюдать принципы ОКП. Чтобы сделать ОКП обязательными в соответствии с требованиями договора, каждая Сторона обязуется выполнить любые дополнительные требования, которые могут понадобиться, для того чтобы ОКП имели силу.

- ii. *Обязательный характер для Сотрудников.* Сотрудники обязаны уважать принципы, установленные в ОКП, как часть их общих обязательств по соблюдению корпоративной политики в соответствии с трудовым договором. Соблюдение ОКП и возможные санкции за любые нарушения ОКП в отношении Сотрудников обеспечиваются внутренним подразделением по нормативно-правовому соответствию. Чтобы сделать ОКП обязательными в соответствии с требованиями договора, каждая Сторона обязуется принять любые дополнительные меры, которые могут понадобиться, для того чтобы ОКП имели обязательную силу в отношении соответствующих Сотрудников.
- iii. *Обязательный характер для Физических лиц (права сторонних бенефициаров).* Все Стороны обязуются предоставлять Физическим лицам права сторонних бенефициаров в соответствии с ОКП в отношении Обработки их Персональных данных. Соответственно, каждая Сторона прямо признает и подтверждает, что Физические лица будут иметь право требовать в принудительном порядке исполнения положений пунктов 3.3, 3.4, 4, 6.1–6.8, 9.1–9.7 и 10.1–10.4 настоящих ОКП в отношении Обработки их Персональных данных и как далее указано в разделе 10.

## **5 Организация по защите данных**

Группа Fresenius создала внутреннюю организацию по защите данных и распределила роли и обязанности среди Сторон для обеспечения адекватной системы управления и поддержки рамочной структуры для обеспечения обработки Персональных данных в соответствии с законом. Группа Fresenius при необходимости будет назначать УЗД и обеспечивать функционирование организации по защите данных для осуществления надлежащего управления и поддержки для каждой Стороны следующим образом:

- Уполномоченный по защите данных (УЗД) контролирует, оценивает и проверяет соблюдение ОКП и Применимого законодательства о защите данных, а также политик и процедур по защите данных. УЗД информирует и консультирует соответствующую Сторону и Сотрудников об их обязательствах в соответствии с ОКП и Применимым законодательством о защите данных, предоставляет консультации по запросу, а в случае Оценки воздействия на защиту данных, расследует нарушения и контролирует устранение таких нарушений, предлагает улучшения системы управления защитой данных и сотрудничает с Надзорными органами и выступает в качестве основного контактного лица для них. УЗД отвечает за объем функций, указанный в его назначении, и подчиняется непосредственно высшему руководству. В этой роли УЗД действует независимо.
- Консультант по защите данных (КЗД) обеспечивает поддержку и консультирование в рамках Организации по защите данных, создает, внедряет и поддерживает в рабочем состоянии систему управления защитой данных, чтобы обеспечить законную Обработку персональных данных и соблюдение ОКП и Применимого законодательства о защите данных. Кроме того, КЗД рассматривает концепции Обработки персональных данных, имеющие отношение к группе Fresenius, проводит оценку рисков нарушения системы защиты данных, консультирует по соглашениям об обработке данных, поддерживает ответственного за этот бизнес-процесс при регистрации действий по обработке данных, консультирует по Оценкам воздействия на защиту данных, готовит ответы на запросы субъектов персональных данных и санкционирует предоставление квалифицированных консультаций МКЗД.

При необходимости КЗД поддерживает по запросу УЗД в его функции контроля и в контактах с Надзорными органами, например, в связи с языковыми вопросами.

- Местный консультант по защите данных (МКЗД) предоставляет консультации и поддержку Ответственному за бизнес или Ответственному за процесс по всем видах деятельности соответствующего местного хозяйственного подразделения Fresenius или по конкретной теме, поддерживает в языковых вопросах, выполняет оценку рисков, имеющих отношение к местному хозяйственному подразделению или к такой теме и рассматривает соответствующие концепции и соглашения по обработке данных, поддерживает Ответственного за бизнес-процесс при организации регистрации деятельности по Обработке данных и документировании соответствующих мер по защите данных.

При необходимости МКЗД поддерживает КЗД и УЗД.

МКЗД назначаются только внутри FK AG.

**С Уполномоченным по защите данных FSE** и всех ее аффилированных лиц в соответствии с разделом 15 и далее Закона Германии об акционерных обществах, за исключением тех, которые относятся к бизнес-сегментам Fresenius Kabi, Fresenius Medical Care, Fresenius Helios и Fresenius Vamed, можно связаться следующим образом:

Уполномоченный по защите данных Fresenius SE и KGaA

Fresenius SE & Co. KGaA  
Else-Kröner-Str. 1  
61352 Bad Homburg v.d.H Germany  
[dataprotectionofficer@fresenius.com](mailto:dataprotectionofficer@fresenius.com)

**С Уполномоченным по защите данных FK AG** и всех ее аффилированных лиц, находящихся в ЕС/ЕЭЗ, в соответствии с разделом 15 и далее Закона Германии об акционерных обществах, относящихся к бизнес-сегменту Fresenius Kabi, можно связаться следующим образом:

Уполномоченный по защите данных Fresenius Kabi

Fresenius Kabi AG  
Else-Kröner-Str. 1  
Bad Homburg v.d.H Germany  
[dataprotectionofficer@fresenius-kabi.com](mailto:dataprotectionofficer@fresenius-kabi.com)

## **6 Принципы защиты Персональных данных по ОКП**

Стороны признают важность конфиденциальности данных Физических лиц. При Обработке Персональных данных, хранящихся Сторонами, должны соблюдаться основные права и свободы Физических лиц, в частности их право на защиту Персональных данных.

В рамках настоящих ОКП каждая Сторона обязуется соблюдать следующие принципы при Обработке Персональных данных:

### **6.1 Законность**

Каждая Сторона обрабатывает Персональные данные только законным образом. Конкретная правовая основа соответствующей деятельности по Обработке данных должна быть соответствующим образом задокументирована. Сторона обрабатывает Персональные данные только на следующих законных основаниях<sup>3</sup>:

---

<sup>3</sup> Ст. 6 ОРЗД

- i. На основании согласия Физического лица, что означает свободно данное, конкретное, информированное и недвусмысленное указание, посредством которого Физическое лицо выражает свое согласие на Обработку его или ее Персональных данных для одной или нескольких указанных целей;
- ii. для исполнения договора, стороной которого является Физическое лицо, или для принятия мер по требованию Физического лица до заключения договора;
- iii. для соблюдения уставных или юридических обязательств группы Fresenius, например, касающихся налогообложения, медицинского оборудования или обязанностей по фармакологическому надзору;
- iv. когда Обработка необходима для выполнения задачи, выполняемой в общественных интересах, или при осуществлении официальных полномочий, предоставленных соответствующей Стороне;
- v. в целях защиты жизненно важных интересов Физического лица или иного физического лица; в
- vi. в целях законного интереса соответствующей Стороны или другой третьей стороны, за исключением случаев, когда Физическое лицо имеет заинтересованность преимущественной силы в том, чтобы его или ее Персональные данные не обрабатывались (см. 9.6).

Обработка Персональных данных, касающихся уголовных судимостей и правонарушений или связанных с ними мер безопасности, основанная на одном из вышеупомянутых правовых оснований, осуществляется только под контролем Надзорного органа или если Обработка разрешена Применимым законодательством о защите данных, предусматривающим соответствующие гарантии прав и свобод Физических лиц. Раздел 3.4 остается в силе без изменений.

Применимое законодательство о защите данных и Применимое законодательство могут предусматривать дополнительные или иные положения в отношении Обработки Персональных данных Сотрудников. В таком случае Стороны обрабатывают Персональные данные Сотрудников в соответствии с такими положениями. Разделы 3.3 и 3.4 остаются в силе без изменений.

Сторона обрабатывает Особые категории Персональных данных только на следующих законных основаниях<sup>4</sup>:

- i. на основании явного согласия Физических лиц на Обработку этих персональных данных для одной или нескольких указанных целей;
- ii. если это необходимо для трудоустройства или целей социального обеспечения;
- iii. в целях защиты жизненно важных интересов Физического лица или другого физического лица, если Физическое лицо физически или юридически неспособно дать согласие;
- iv. если Персональные данные были явно обнародованы Физическим лицом;
- v. если это необходимо для инициирования и ведения судебных исков или для защиты по ним;
- vi. если это необходимо для значительного общественного интереса, соразмерного преследуемой цели, с соблюдением сущности права на защиту данных и указанием подходящих и конкретных мер для защиты основных прав и интересов Физических лиц;
- vii. если это необходимо в целях профилактической или профессиональной медицины, для оценки работоспособности Сотрудников, медицинской диагностики, предоставления

---

<sup>4</sup> Ст. 9 ОРЗД

медицинской или социальной помощи или лечения, или для управления системами и услугами здравоохранения или социальной помощи;

- viii. если это необходимо по причинам общественного интереса в области государственного (на трансграничной основе) здравоохранения, такого как обеспечение высоких стандартов качества и безопасности медицинской помощи, а также лекарственных средств или медицинского оборудования, обеспечение прав Физических лиц, в частности, профессиональной тайны; или
- ix. если это необходимо для целей архивирования в общественных интересах, в целях научных или исторических исследований, или в статистических целях, при условии, что Обработка соблюдает сущность права на защиту данных и принимает подходящие и конкретные меры для защиты основных прав и интересов Физических лиц, а также принципов, заложенных в настоящих ОКП.

## **6.2 Прозрачность и справедливость**

Каждая Сторона обрабатывает Персональные данные справедливо и прозрачно<sup>5</sup>, это означает, что Физическое лицо, как правило, заранее адекватно проинформировано<sup>6</sup> об Обработке своих Персональных данных, и ему предоставлена информация о правах Субъектов персональных данных в соответствии с Разделом 9, а также любых других правах, предоставляемых ему по Применимому законодательству о защите данных, в отношении его Персональных данных (см. раздел 9 ниже).

Если Персональные данные получены не от Физического лица, информация будет предоставлена:

- i. в течение разумного периода после получения Персональных данных, но не позднее чем в течение одного месяца; принимая во внимание конкретные обстоятельства, при которых обрабатываются Персональные данные;
- ii. если Персональные данные должны использоваться для связи с Физическим лицом, самое позднее на момент первого сообщения этому Физическому лицу; или
- iii. если предусмотрено раскрытие другому получателю, не позднее момента первого раскрытия Персональных данных.

Любая информация, предоставляемая Физическим лицам, или любое общение с Физическим лицом, связанное с Обработкой его Персональных данных, должно быть кратким, прозрачным, всеобъемлющим и в легкодоступной форме, с использованием ясного и простого языка.

### **6.2.1 Обязательная информация**

Такая прозрачная информация для Физического лица включает следующее:

- i. идентификация и контактные данные Стороны и, если применимо, представителя хозяйственного подразделения Fresenius;
- ii. контактные данные Уполномоченного по защите данных, если он назначен;
- iii. цели Обработки Персональных данных, а также правовые основания Обработки;
- iv. если Обработка основана на законном интересе, преследуемые Стороной или третьей стороной законные интересы;
- v. получатели или категории получателей Персональных данных (при наличии);
- vi. при любой Передаче Персональных данных в страну за пределами ЕС/ЕЭЗ или международной организации, правовая основа, на которой основана такая Передача,

---

<sup>5</sup> Ст. 5, п. 1 (а) ОРЗД

<sup>6</sup> Ст. 13 и ст. 14 ОРЗД

включая ссылку на соответствующие или подходящие меры защиты и средства, с помощью которых можно получить их копию, или где они доступны.

#### 6.2.2 Дополнительная информация, которая должна быть предоставлена

Для обеспечения справедливой и прозрачной Обработки будет предоставляться следующая дополнительная информация:

- i. период, в течение которого будут храниться Персональные данные;
- ii. права Физических лиц, перечисленные в разделе 9 настоящих Обязательных корпоративных правил;
- iii. если Обработка основана на согласии, наличие права отозвать согласие в любое время, которое будет иметь силу только для будущей Обработки Персональных данных;
- iv. право подать претензию в Надзорный орган;
- v. существование любого автоматизированного принятия решений, включая составление профиля, и содержательную информацию о задействованной логике, а также о значении и предполагаемых последствиях такой обработки.
- vi. является ли предоставление Персональных данных законодательным или договорным требованием, или требованием, необходимым для заключения договора, а также обязано ли Физическое лицо предоставлять Персональные данные, и о возможных последствиях непредоставления таких Персональных данных;

#### 6.2.3 Дополнительная информация, которая должна быть предоставлена в том случае, если данные получены от третьей стороны.

В случае получения Персональных данных от третьей стороны, не от Физического лица, Сторона должна предоставлять следующую дополнительную информацию:

- i. категории Обрабатываемых Персональных данных; и
- ii. источник Персональных данных.

### 6.3 Ограничение целей

Любая Сторона будет обрабатывать Персональные данные только для указанных целей, для которых собираются Персональные данные. Любая Сторона не будет обрабатывать Персональные данные для целей, несовместимых с первоначальными целями, за исключением случаев, когда изменение цели разрешено законодательством ЕС о защите данных. Принимаются дополнительные меры для защиты прав и свобод Физического лица, такие как согласие соответствующих затрагиваемых Физических лиц, ограничение доступа к Персональным данным, дополнительные меры контроля соблюдения конфиденциальности и безопасности, предоставление информации Физическому лицу.

Как правило разрешенными целями дальнейшей Обработки, которые считаются совместимыми с первоначальной целью, являются:

- i. архивирование;
- ii. внутренний аудит и расследования.

Чтобы точно определить, совместима ли Обработка для другой цели с целью, для которой Персональные данные первоначально собраны, среди прочего, необходимо принимать во внимание следующее:

- i. наличие связи между целями, для которых были собраны Персональные данные, и целями предполагаемой дальнейшей обработки;
- ii. контекст, в котором были собраны персональные данные, в частности, отношения между Физическими лицами и соответствующей Стороной;

- iii. характер Персональных данных, в частности, обрабатываются ли Особые категории Персональных данных в соответствии со статьей 9 ОРЗД или обрабатываются Персональные данные, связанные с уголовными судимостями и правонарушениями, в соответствии со статьей 10 ОРЗД;
- iv. возможные последствия предполагаемой дальнейшей Обработки для Физических лиц;
- v. наличие соответствующих мер защиты, которые могут включать шифрование или псевдонимизацию.

(Местный) консультант по защите данных сможет дать указания относительно того, разрешено ли и когда такое изменение.

В случае разрешенного изменения цели Физические лица должны быть проинформированы о любых таких изменениях в соответствии с разделом 6.2 до того, как Персональные данные будут обработаны для такой другой цели.

#### **6.4 Минимизация данных**

Любая Сторона собирает и обрабатывает Персональные данные только в объеме, необходимом для деловых целей и о которых проинформирован субъект Персональных данных (первоначальная цель) или тех, которые совместимы с этими первоначальными целями в соответствии с разделом 6.3. Любая Сторона не будет собирать или обрабатывать Персональные данные, которые являются чрезмерными или не имеют отношения к цели, для которой необходимы Персональные данные.

#### **6.5 Точность**

Группа Fresenius будет поддерживать точность и актуальность Персональных данных. Каждая Сторона будет внедрять процедуры, обеспечивающие безотлагательное удаление, исправление или обновление неточных данных на протяжении их соответствующего жизненного цикла.

#### **6.6 Ограничение хранения**

Каждая Сторона не будет хранить Персональные данные больше, чем это необходимо для целей, для которых Персональные данные обрабатываются, за исключением случаев, когда хранение Персональных данных предусмотрено законом. Если Персональные данные необходимо сохранить по причинам, отличным от их первоначальной цели (например, потому, что действующее законодательство требует хранить данные в течение более длительного периода времени), доступ к ним будет ограничен. Если у Стороны больше нет законного или правомерного интереса хранить Персональные данные, Персональные данные должны быть анонимизированы или надежно удалены.

#### **6.7 Безопасность, целостность и конфиденциальность**

##### **6.7.1 Технические и организационные меры безопасности**

Каждая Сторона примет соответствующие технические и организационные меры для защиты передаваемых, хранимых или иным образом обрабатываемых Персональных данных от случайного или незаконного уничтожения, потери, изменения, несанкционированного раскрытия или доступа. Каждая Сторона будет учитывать, в частности, новейшие разработки, затраты на реализацию, а также характер, объем, контекст и цели Обработки, кроме того риски различной вероятности и серьезности для прав и свобод Физических лиц при реализации таких технических и организационных мер с учетом конфиденциальности, целостности и доступности хранимых Персональных данных, путем установки и обслуживания систем и служб Обработки данных, настроенных так, чтобы оставаться устойчивыми к кибератакам и угрозам ИТ-безопасности, включая, среди прочего, в зависимости от обстоятельств следующее:

- i. псевдонимизация и шифрование Персональных данных;



- ii. способность обеспечивать непрерывную конфиденциальность, целостность, доступность и отказоустойчивость систем и услуг обработки;
- iii. возможность своевременного восстановления наличия и доступа к Персональным данным в случае физического или технического инцидента;
- iv. процесс регулярного тестирования, анализа и оценки эффективности технических и организационных мер по обеспечению безопасности Обработки.

#### 6.7.2 Уведомление о нарушениях мер защиты в отношении Персональных данных

Каждая Сторона обязуется уведомлять о любом нарушении безопасности, ведущем к любому случайному или незаконному уничтожению, или случайной утрате, изменению, несанкционированному раскрытию или доступу к Персональным данным Организацию по защите данных FSE и FK AG, которая, в свою очередь, должна информировать штаб-квартиру ЕЭЗ. Кроме того, в случае такого нарушения мер защиты в отношении Персональных данных существуют следующие обязательства по уведомлению:

- i. любая Сторона, подпадающая под действие ОРЗД и действующая в качестве Контролера, должна уведомить Надзорный орган о любом нарушении мер защиты Персональных данных, которое может привести к риску для затронутых Физических лиц, без неоправданной задержки и, если это возможно, не позднее семидесяти двух (72) часов после того, как стало известно о нарушении мер защиты Персональных данных;
- ii. любая другая Сторона, действующая в качестве Контролера, должна уведомить Соответствующий надзорный орган о любом нарушении мер защиты Персональных данных, которое может привести к риску для затронутых Физических лиц, без неоправданной задержки и, если это возможно, не позднее, чем через семьдесят два (72) часа после того, как стало известно о нарушении мер защиты Персональных данных;
- iii. любая Сторона, действующая в качестве Обработчика для другой Стороны, должна уведомить о любом нарушении мер защиты Персональных данных соответствующую Сторону, действующую в качестве Контролера, и соответствующего МКЗД.
- iv. если нарушение мер защиты Персональных данных может привести к высокому риску для прав и свобод затронутых Физических лиц, соответствующая Сторона, действующая в качестве Контролера, должна без неоправданной задержки сообщить об утечке персональных данных затронутым Физическим лицам.

Каждая Сторона документирует такое произошедшее нарушение безопасности (включая факты, связанные с нарушением, его последствиями и предпринятыми мерами по устранению) и после консультации с Организацией по защите данных FSE и FK AG предоставляет такую документацию Надзорным органам.

#### 6.8 Подотчетность

Каждая Сторона должна придерживаться принципов, изложенных выше, и демонстрировать соблюдение ОКП, и для этого создает и ведет надлежащую документацию, в том числе:

- i. Ведение отчетности о деятельности по Обработке данных с указанием следующего:
  - имя и контактные данные Контролера и, если применимо, совместного контролера, представителя Контролера и Уполномоченного по защите данных;
  - цели Обработки;
  - описание категорий Физических лиц и категорий Персональных данных;
  - категории получателей, которым Персональные данные были или будут раскрыты, включая получателей в третьих странах или международных организациях;
  - где это применимо, Передачи Персональных данных за пределы ЕС или международной организации, включая соответствующие меры защиты, как определено в разделе 6.8.2;



## Обязательные корпоративные правила (ОКП)

- по возможности, предусмотренные сроки удаления различных категорий Персональных данных;
- по возможности общее описание технических и организационных мер безопасности, указанных в разделе 6.7.

Эта отчетность должна вестись в письменной форме, в том числе в электронной форме, и предоставляться Надзорным органам по запросу.

- ii. Реализация надлежащих технических и организационных мер, направленных на реализацию принципов защиты данных и облегчение соблюдения требований, установленных ОКП, на практике (защита данных по плану и по умолчанию).
- iii. Проведение Оценки воздействия на защиту данных, как указано в разделе 8.

### 6.8.1 Привлечение Обработчиков

Каждая Сторона будет привлекать Обработчиков только при условии достаточных гарантий для реализации надлежащих технических и организационных мер таким образом, чтобы Обработка соответствовала требованиям ОКП и Применимого законодательства о защите данных (в частности, ОРЗД) и обеспечивала защиту прав Физических лиц.

Любая Обработка Обработчиком регулируется договором или другим юридическим актом, который имеет обязательную силу для Обработчика в отношении Контролера, и предусматривает, среди прочего:

- i. что Обработчик должен Обрабатывать Персональные данные исключительно в соответствии с инструкциями, полученными от Контролера данных;
- ii. что Обработчик должен осуществлять надлежащие технические и организационные меры для защиты Персональных данных;
- iii. что Обработчик гарантирует, что лица, уполномоченные на Обработку Персональных данных, взяли на себя обязательство соблюдать конфиденциальность или находятся под соответствующим законодательным обязательством по соблюдению конфиденциальности;
- iv. что Обработчик должен удалить или вернуть все Персональные данные после окончания оказания услуг, связанных с Обработкой, и удалить существующие копии;
- v. что Обработчик может привлекать только субподрядчиков, предоставляющих достаточные гарантии для реализации надлежащих технических и организационных мер таким образом, чтобы Обработка соответствовала требованиям ОКП и Применимого законодательства о защите данных, на основе письменных договорных актов, устанавливающих тот же уровень обязательств по защите данных для субподрядчиков, который установлен между Стороной и Обработчиком;
- vi. что Обработчик будет поддерживать соответствующую Сторону в выполнении ее обязательств по реагированию на запросы Физических лиц;
- vii. что Обработчик предоставляет всю информацию, необходимую для демонстрации соблюдения настоящего раздела, а также позволяет проводить контрольные проверки и содействует в их проведении, включая проверки, проводимые соответствующей Стороной или другим согласованным аудитором;
- viii. что Обработчик будет помогать соответствующей Стороне в обеспечении соблюдения обязательств, указанных в разделах 6.7 и 7.

### 6.8.2 (Последующие) Передачи Персональных данных

Стороны будут принимать меры для адекватной защиты Передач Персональных данных Сторонним получателям, расположенным за пределами ЕЭЗ, в соответствии с настоящими ОКП.

Персональные данные могут быть переданы Стороннему получателю за пределами ЕЭЗ только в случае соблюдения хотя бы одного из следующих условий:

- i. Сторонний получатель находится в стране, которая была признана Европейской комиссией как предлагающая адекватный уровень защиты Персональных данных (так называемые страны «Белого списка»), и, насколько применимо, Сторонний получатель выполняет все дополнительные требования с соответствующей соразмерностью; или
- ii. если Сторонний получатель обеспечил соответствующие меры защиты, и при условии, что Физическим лицам доступны законодательно предусмотренные права и эффективные средства правовой защиты Физических лиц; например, на основании стандартных договорных положений, принятых Европейской Комиссией; или

В отступление от вышеупомянутых альтернатив Персональные данные также могут быть переданы в случае применения одного из следующих исключений:

- i. Физическое лицо дало свое явное согласие на Передачу своих Персональных данных после того, как было проинформировано о возможных рисках такой передачи; или
- ii. Передача Персональных данных необходима (i) для исполнения договора с Физическим лицом или реализации преддоговорных мер, предпринимаемых по запросу Физического лица; или (ii) для выполнения или заключения договора, заключаемого в интересах Физического лица между Контролером и другим физическим или юридическим лицом; или
- iii. Передача Персональных данных необходима (i) для защиты жизненно важных интересов Физического лица или других лиц (т.е. в вопросах жизни или смерти), когда Физическое лицо физически или юридически неспособно дать согласие, или (ii) чтобы позволить Fresenius инициировать и вести судебный иск или для защиты по нему, или (iii) по веским причинам, преследующим общественный интерес; или
- iv. Передача осуществляется из реестра, который в соответствии с законодательством ЕС или Государства-члена предназначен для предоставления информации общественности и открыт для ознакомления либо для общественности в целом, либо для любого лица, которое может продемонстрировать законный интерес, но только в той степени, насколько выполняются условия для ознакомления, предусмотренные законодательством ЕС или Государства-члена, в каждом конкретном случае.

Если ни одно из вышеперечисленных условий не соблюдено, и Передача не является повторной, касается только ограниченного числа субъектов Персональных данных, необходима для целей обеспечения законных интересов и не перекрывается интересами или правами и свободами субъекта Персональных данных, отправляющая Сторона должна оценить обстоятельства, связанные с Передачей данных, и обеспечить соответствующие меры защиты в отношении обеспечения конфиденциальности Персональных данных, а также должна проинформировать Соответствующий Надзорный орган о Передаче.

Во избежание сомнений, вышеупомянутые условия также применяются к любой Последующей Передаче Персональных данных Стороной, находящейся за пределами ЕС/ЕЭЗ, Стороннему получателю, находящемуся за пределами ЕС/ЕЭЗ, куда первоначально были переданы соответствующие Персональные данные Стороной, находящейся в ЕС/ЕЭЗ.

## **7 Оценка рисков в защите данных**

Каждая Сторона проводит оценку рисков в защите данных для любой деятельности по Обработке данных, связанной с Персональными данными. Оценка рисков в защите данных это формальный процесс оценки влияния любой деятельности по Обработке данных на права и свободы соответствующих заинтересованных Физических лиц (Риски конфиденциальности). Оценка рисков проводится посредством подробного анализа деятельности по Обработке данных и служит для определения:

- i. Рисков конфиденциальности для Физических лиц, возникающих в результате деятельности по Обработке данных;
- ii. применимых требований, вытекающих из ОКП и Применимого законодательства о защите данных; и
- iii. подходящих мер для выполнения этих требований и снижения выявленных Рисков конфиденциальности.

В частности, каждая Сторона перед Передачей Персональных данных другой Стороне, находящейся за пределами ЕС/ЕЭЗ, должна оценить, способна ли последняя на практике соблюдать гарантии, предусмотренные в ОКП, принимая во внимание контекст и цель передачи данных, возможный конфликт с Применимым законодательством или Применимым законодательством о защите данных в третьей стране, в отношении основных прав Физических лиц. Если это не так, Стороны должны оценить, могут ли они обеспечить дополнительные технические, организационные или договорные меры/средств контроля для обеспечения практически эквивалентного уровня защиты, предусмотренного в ЕС. Если такие меры не могут быть осуществлены, Сторона не выполняет Передачу. Если Сторона уже осуществляет Передачу Персональных данных, передача должна быть приостановлена или прекращена. Уже переданные Персональные данные или их копии должны быть возвращены отправляющей Стороне или полностью уничтожены получателем. Любые оценки, полученные в соответствии с настоящим пунктом, должны регулярно пересматриваться.

Оценка рисков состоит из следующих основных этапов:

- iv. Предварительная оценка

Предварительная оценка определяет присущие Риски конфиденциальности, возникающие в результате деятельности по Обработке данных, и квалифицирует их как высокие, средние или низкие. Результаты Предварительной оценки определяют дальнейшие шаги по Оценке рисков.

- v. Оценка средств контроля

В рамках Оценки средств контроля определяются и документируются меры/средства контроля, которые должны быть реализованы или необходимые для реализации, в соответствии с тремя уровнями серьезности, для смягчения присущих рисков, определенных предварительной оценкой и, где это применимо, из-за высокого риска, определенного ОВЗД, а также для выполнения требований ОКП и Применимого законодательства о защите данных.

- vi. Оценка адекватности средств контроля защиты данных

Адекватность реализованных или подлежащих реализации технических, организационных или договорных мер оценивается для определения остаточных Рисков конфиденциальности.

- vii. Отчетность о рисках

Выявленные пробелы в контроле и потенциальные остаточные риски должны быть задокументированы и включены в отчет. Пробелы и риски должны быть устранены, а технические и организационные меры для их снижения должны быть реализованы до начала деятельности по Обработке данных.

Если Предварительная оценка выявляет высокий Риск конфиденциальности, соответствующим (Местным) консультантом по обеспечению конфиденциальности данных должна быть проведена дополнительная Оценка воздействия на защиту данных (ОВЗД) и затем она должна быть одобрена соответствующим Уполномоченным по защите данных.

## **8 Оценка воздействия на защиту данных<sup>7</sup>**

Каждая Сторона проводит Оценку воздействия на защиту данных (ОВЗД) до начала Обработки, если Обработка Персональных данных может привести к высокому риску для прав и свобод Физических лиц. Необходима консультация соответствующего Уполномоченного по защите данных.

Чтобы оценить необходимость ОВЗД Сторона должна принимать во внимание вид Обработки, использование новых технологий, а также характер, объем, контекст и цели Обработки. Если ОВЗД выявляет высокий риск конкретной деятельности по Обработке данных, ответственная Сторона должна предпринять адекватные меры для снижения таких рисков до начала Обработки. Если ОВЗД выявит, что Обработка все равно приведет к высокому риску даже с учетом мер, принятых для снижения риска, перед Обработкой следует проконсультироваться с Соответствующим Надзорным органом.

ОВЗД, в частности, требуется в следующих случаях:

- i. систематическая, обширная и автоматизированная Обработка Персональных данных, включая создание профилей и принятие решений, которые оказывают существенное влияние на Физических лиц, или
- ii. крупномасштабная Обработка Особых категорий Персональных данных или относящихся к уголовным судимостям и правонарушениям.

## **9 Права Физических лиц<sup>8</sup>**

Каждая Сторона должна обеспечить Физическим лицам возможность осуществлять следующие права.

Каждая Сторона должны информировать получателей, если и в той степени, насколько Физическое лицо потребует исправления, удаления или ограничения Персональных данных, за исключением случаев, когда это окажется невозможным или потребует непропорциональных усилий. Стороны должны информировать Физическое лицо о получателях по запросу Физического лица. Любой запрос, который Сторона может получить от Физического лица в отношении вышеупомянутых ее/его прав, должен обрабатываться в соответствии с процедурой рассмотрения претензий, описанной в разделе 10.2 ОКП.

### **9.1 Право на доступ к Персональным данным**

Физическое лицо имеет право запросить доступ/получение информации о своих Персональных данных, цели Обработки, соответствующих категориях Персональных данных, получателях Персональных данных, сроках хранения Персональных данных или их критериях, наличии права требовать исправления или удаления Персональных данных или ограничения Обработки Персональных данных, касающихся Физического лица, или возражать против такой Обработки, право подать претензию в Надзорный орган и источник Персональных данных, если Персональные данные собираются не у субъекта Персональных данных, любое существование автоматизированного принятия решений, включая создание профиля, любую Передачу в страну за пределами ЕС/ЕЭЗ, а также получение копии Персональных данных, подвергающихся Обработке (см. также раздел 6.2).

### **9.2 Право на исправление Персональных данных**

Физическое лицо имеет право потребовать исправления касающихся его или ее неточных или неполных Персональных данных, обрабатываемых Стороной, а также дополнения неполных Персональных данных.

---

<sup>7</sup> Ст. 35 ОРЗД

<sup>8</sup> Глава III ОРЗД

### **9.3 Право на удаление Персональных данных**

Физическое лицо имеет право потребовать удаления своих Персональных данных, обрабатываемых Стороной, при условии и в той степени, насколько соблюдено одно из следующих условий: (i) Персональные данные больше не являются необходимыми для целей, для которых они собирались или иным образом обрабатывались, (ii) Физическое лицо отзывает согласие, на котором основана Обработка, и если нет другого законного основания для Обработки, (iii) Физическое лицо возражает против Обработки соответственно, и нет никаких приоритетных законных оснований для Обработки, или Физическое лицо возражает против Обработки для целей прямого маркетинга, которая включает создание профиля, в той степени, насколько она относится к такому прямому маркетингу, (iv) Персональные данные были обработаны незаконно, или (v) Персональные данные должны быть удалены в целях соблюдения обязательства, установленного в Применимом законодательстве, действию которого подчиняется контролер. Необходимо соблюдать существующие обязательства по хранению данных и/или конфликту интересов; применяется раздел 3.4.

### **9.4 Право на ограничение Обработки Персональных данных**

Физическое лицо имеет право потребовать ограничения Обработки его или ее Персональных данных, если либо (i) точность Персональных данных оспаривается Физическим лицом, либо Физическое лицо возражает против Обработки (см. ниже раздел 9.6) на срок, позволяющий соответствующей Стороне проверить точность Персональных данных или проверить, имеет ли соответствующая Сторона законные основания, которые имеют преимущественную силу над законными основаниями Физического лица; или (ii) Обработка является незаконной, соответственно, больше не требуется для соответствующих преследуемых целей, но Физическое лицо возражает против удаления Персональных данных и вместо этого требует ограничения их использования (например, если Персональные данные необходимы для инициирования и ведения судебных исков или защиты по ним).

### **9.5 Право на получение Персональных данных в портативном формате и на передачу Персональных данных**

Если Персональные данные были предоставлены Физическим лицом, и Обработка осуществляется на основании согласия Физического лица или на основании договора с Физическим лицом, и Обработка осуществляется автоматизированными средствами, Физическое лицо имеет право на получение своих Персональных данных в обычно используемом и в машиночитаемом формате и на беспрепятственную передачу этих данных (насколько это технически возможно), с тем чтобы Физическое лицо могло использовать аналогичные услуги от другого Контролера.

### **9.6 Право возражения против обработки персональных данных**

Физическое лицо имеет право на основаниях, связанных с его или ее конкретной ситуацией, возражать против Обработки своих Персональных данных, исходя из законных интересов Сторон или третьих лиц, или общественных интересов (это право не применяется, если положение закона требует Обработки Персональных данных). Обработка должна быть прекращена, если соответствующая Сторона не продемонстрирует убедительные законные основания для Обработки, которые имеют преимущественную силу над интересами, правами и свободами Физического лица, или для инициирования и ведения судебных исков или для защиты по ним.

Кроме того, Физическое лицо имеет право возражать против Обработки относящихся к нему или к ней Персональных данных в целях прямого маркетинга, включающих создание профиля в той степени, насколько она связана с таким прямым маркетингом.

### **9.7 Право не подвергаться автоматическому принятию решений**

Физические лица также имеют право не подвергаться решению Стороны, основанному исключительно на автоматизированной Обработке, включая создание профиля, которое может привести к юридическим или аналогичным значительным последствиям для Физического лица, если только это решение:

- i. не является необходимым для заключения или исполнения договора между Физическим лицом и соответствующей Стороной и не основано на явно выраженном согласии Физического лица, при условии, что соответствующая Сторона приняла соответствующие меры для защиты прав, свобод и законных интересов Физического лица, по крайней мере, право на человеческое участие от Стороны, чтобы выразить свою точку зрения и оспорить решение; или
- ii. не разрешено Применимым законодательством, действию которого подчиняется соответствующая Сторона, и которое также устанавливает подходящие меры для защиты прав, свобод и законных интересов Физического лица. Раздел 3.4 применяется без изменений.

С этой целью Особые категории Персональных данных могут обрабатываться исключительно либо в том случае, если Физическое лицо дало свое явное согласие, либо если это разрешено Применимым законодательством, действию которого подчиняется соответствующая Сторона, и такая Обработка должна быть соразмерной преследуемой цели, соблюдать существо права на защиту данных и предусматривать подходящие и конкретные меры для защиты основных прав и интересов такого Физического лица.

## **10 Соблюдение ОКП**

### **10.1 Доступ к ОКП**

Каждая Сторона сделает полную версию ОКП, особенно те разделы, которые предоставляют права Физическим лицам, в частности разделы 3.3, 3.4, 4, 6.1–6.8, 9.1–9.7 и 10.1–10.4 ОКП, доступной для физических лиц вне компании через интернет на специальном вебсайте Группы Fresenius. Полная версия ОКП также должна быть доступна внутри компании через вебсайты внутренней сети Группы Fresenius. Физические лица также могут получить доступ к полным версиям ОКП, одобренным для публикации, обратившись к соответствующему Уполномоченному по защите данных или к любому члену Организации по защите данных.

### **10.2 Обработка претензий в отношении ОКП**

Каждое Физическое лицо имеет право заявить о нарушении ОКП, урегулировать свои права Физического лица, изложенные в разделе 9 настоящих ОКП, требовать соблюдения любого другого права по ОКП или направлять любой другой запрос в Организацию по защите данных. Группа Fresenius внедрит процедуры, обеспечивающие рассмотрение таких претензий.

Претензии означают любой отчет, в котором заявляется о потенциальном нарушении ОКП, Применимого законодательства о защите данных, приказов Надзорных органов, внутренних политик и руководств или добровольных обязательств, касающихся защиты данных. В то время как запросы в отношении прав субъектов Персональных данных означают все запросы Физических лиц, отсылающие к правам, предоставляемым в соответствии с разделом 9 настоящих ОКП и поданные в соответствии с процедурой обработки запросов субъектов Персональных данных.

Любые такие претензии могут быть поданы по нескольким каналам для подачи претензий. Запрос можно подать, например, по телефону или в письменной форме, например, по электронной почте или письмом, или устно, обратившись к соответствующему Уполномоченному по защите данных, соответствующему (местному) Консультанту по защите данных или на горячую линию по вопросам обеспечения нормативно-правового соответствия. Соответствующие каналы связи опубликованы на вебсайтах компании Fresenius в интернете и во внутренней сети группы Fresenius, где предоставлена вся необходимая информация (<https://www.fresenius.com/compliance> – отчеты о потенциальных случаях несоответствия нормативно-правовым требованиям или <https://www.fresenius-kabi.com/responsibilities/compliance>).



Претензии, являющиеся оскорбительными, особенно если они явно необоснованы или чрезмерны, в частности, из-за их повторяющегося характера, или которые представляют собой оскорбительные действия в отношении компании Fresenius или любого Сотрудника, будут отклонены. В таком случае Физическому лицу будет предоставлено письменное объяснение причины отказа и предоставлено право на обжалование.

В случае, если претензия будет признана обоснованной, Сторона предпримет адекватные действия для рассмотрения претензии, приложив разумные усилия для устранения или исправления ситуации, которая послужила причиной подачи претензии. Физическое лицо будет уведомлено в письменной форме о том, что адекватные действия по рассмотрению претензии будут или были приняты. В любом случае Физическое лицо будет уведомлено о его или ее праве подать иск в суд или претензию в Надзорный орган в соответствии с разделом 10.3 в том случае, если он или она не удовлетворены рассмотрением своей претензии.

В отношении запросов субъектов Персональных данных Уполномоченный по защите данных при поддержке (Местного) Консультанта по защите данных постарается, где это возможно, дать Физическому лицу ответ по существу в течение одного (1) календарного месяца с момента получения претензии. Если невозможно предоставить ответ по существу в течение одного (1) календарного месяца, например, из-за характера претензии, Физическое лицо будет уведомлено об этом соответствующим Уполномоченным по защите данных при поддержке соответствующего (местного) Консультанта по защите данных с указанием предварительной оценки того, когда можно ожидать получения ответа по существу. Ответ по существу должен быть предоставлен не позднее, чем через три (3) месяца после получения претензии.

Кроме того, контактные данные Уполномоченного по защите данных и других членов Организации по защите данных указаны выше в разделе 5 настоящих Обязательных корпоративных правил.

Организация по защите данных документирует действия Физических лиц в соответствии с настоящим разделом 10.2.

### **10.3 Ответственность и правоприменение**

Физические лица, которые пострадали или понесли ущерб в результате Обработки их соответствующих Персональных данных, которая является незаконной или противоречит обязательным к исполнению частям ОКП, как указано в разделе 4, произведенной либо Стороной, либо привлеченным Обработчиком, либо субподрядчиком, имеют право возбудить иски или разбирательства для обеспечения соблюдения этих частей ОКП и, если применимо, получить компенсацию в компетентном суде либо в стране, где учреждена Сторона, либо в Бад-Хомбурге, Германия, где учреждены FSE и FK AG, либо в месте постоянного проживания соответствующего Физического лица, а также в Надзорных органах, в частности, в стране постоянного проживания или места работы Физического лица, или места заявляемого нарушения, например, путем подачи претензии.

В случае доказанных нарушений подлежащих обязательному исполнению частей ОКП, как указано в разделе 4, Сторонами, учрежденными за пределами ЕС/ЕЭЗ, FSE принимает на себя ответственность и несет ответственность за любой ущерб, причиненный таким нарушением ОКП, и соглашается принять любые соответствующие меры для исправления действия Сторон, учрежденных за пределами ЕС/ЕЭЗ, и выплатить компенсацию за любой материальный или нематериальный ущерб, причиненный Физическому лицу в результате любого такого нарушения. Прежде чем выплатить какую-либо компенсацию или сделать какие-либо заявления в отношении субъекта Персональных данных, FSE незамедлительно уведомит заинтересованную Сторону о требовании, чтобы позволить заинтересованной Стороне запросить охранный судебный приказ или другое надлежащее средство правовой защиты. FSE имеет право самостоятельно требовать охранный судебный приказ или другого надлежащего средства правовой защиты от заявляемого нарушения.



Если Физические лица могут доказать, что они понесли ущерб, и последовательно изложить факты, которые показывают вероятность заявляемых нарушений, соответственно, что ущерб возник из-за заявляемого нарушения ОКП, FSE должна доказать в противоположность Физическому лицу, что Сторона, причинившая ущерб, не несет ответственности за нарушение ОКП, повлекшее за собой такой ущерб, или что не было такого нарушения. Сторона, причинившая ущерб, обязана оказать FSE разумную помощь для своевременного реагирования на такие претензии или запросы.

Любая Сторона, расположенная за пределами ЕС/ЕЭЗ, будет выполнять любой запрос или приказ Надзорного органа, имеющий обязательную силу для Стороны, как если бы Сторона была учреждена в ЕС/ЕЭЗ.

#### **10.4 Сотрудничество с надзорными органами**

Каждая Сторона обязана (i) сотрудничать с Соответствующими Надзорными органами, (ii) соблюдать рекомендации по любому вопросу, связанному с толкованием настоящих ОКП, (iii) соглашаться на проверку со стороны Соответствующих Надзорных органов. По запросу Соответствующего Надзорного органа соответствующий Уполномоченный по защите данных должен предоставлять копию соответствующего акта проверки, созданного в рамках программы контроля, как описано в разделе 10.6.

#### **10.5 Обучение**

Каждая Сторона регистрирует для участия и обязет своих Сотрудников, участвующих в Обработке Персональных данных или разработке инструментов, используемых для Обработки Персональных данных, пройти обучение по ОКП и Применимому законодательству о защите данных, а также регулярно повторять такое обучение. Общее обучение проводится не реже одного раза в два года для всех соответствующих Сотрудников. Кроме того, проводится специальное, в зависимости от выполняемых функций, обучение (например, специальные информационные и коучинговые занятия или семинары) с учетом конкретных потребностей определенных должностей/лиц, например, членов Организации по защите данных FSE и FK AG.

Обучение является обязательным для соответствующих Сотрудников. После приглашения по электронной почте на обучение Сотруднику предоставляется заранее определенное время для его завершения. Сотрудники, не прошедшие обучение в указанное время, получают напоминание. Кроме того, руководитель Сотрудника получает уведомление с напоминанием, которое будет рассылаться ежемесячно до завершения обучения. Сотрудник, не прошедший соответствующее обучение после двух напоминаний, может быть подвергнут (дисциплинарному) взысканию в соответствии с действующим трудовым законодательством.

В большинстве случаев обучение будет проводиться через платформу электронного обучения. Как правило, обучение заканчивается проверкой, помогающей закрепить понимание содержания, например, с помощью теста с множественным выбором или с пробелами для ввода текста.

#### **10.6 Контроль**

Стороны реализуют и обязуются вести программу контроля, охватывающую области, связанные с защитой данных у каждой Стороны, в частности все аспекты, регулируемые ОКП. Все Стороны обязуются регулярно подвергаться контролю для оценки и проверки соблюдения ОКП, а также внедрять адекватные и достаточные механизмы для устранения несоответствий Стороны требованиям ОКП. Будут проводиться плановые контрольные проверки, которые дополняются специальными контрольными проверками в случае, если этого потребует Организация по защите данных или руководство Сторон.

Плановые контрольные проверки должны, *среди прочего*, охватывать следующие области: (i) Управление защитой данных (например, насколько выполняется требования ОКП о наличии и действии наборов правил и процедур по защите данных и т. д.), (ii) безопасность Персональных данных (например, используются ли технические и организационные меры

для обеспечения адекватной безопасности обрабатываемых Персональных данных и т. д.), (iii) Обучение и осведомленность (например, проведение и посещаемость обучающих мероприятий по защите данных и т. д.), (iv) Запросы Физических лиц и Надзорных органов (например, работающие процедуры для ответов на запросы Физических лиц, а также для связи с Надзорными органами и т. д.), (v) Передача данных: соблюдение ОКП, в частности, в отношении потенциального конфликта с Применимым законодательством и т. д.

Частота и последовательность плановых контрольных проверок будут определяться ежегодно в плане проверок на основе рисков, связанных с соответствующими Передачами, принимая во внимание, среди прочего, следующие аспекты: (i) объем Персональных данных, (ii) конфиденциальность Персональных данных (в том числе, затрагиваются ли Особые категории Персональных данных), (iii) типы Физических лиц, (iv) степень критичности для внутренних операций, а также (v) потенциальное воздействие на Физическое лицо, в частности, на основе проведенных Оценок воздействия на защиту данных (см. раздел 8). Число Сторон, прошедших проверку в течение года, не должно опускаться ниже пяти.

Объем *специальных* контрольных проверок определяется Организацией по защите данных или руководством Сторон в каждом конкретном случае.

Результатом каждой контрольной проверки будет акт проверки, который будет официально направлен всем проверяемым организациям, соответствующему совету или высшему руководству контролирующего предприятия, МКЗД, соответствующему Управляющему по защите данных и Директору по обеспечению нормативно-правового соответствия Сторон. Организация по защите данных будет отслеживать любые проведенные контрольные проверки, чтобы оценить, были ли предложенные корректирующие действия реализованы надлежащим образом, и документировать любые результаты в акте проверки. Каждая Сторона должна предоставлять акты проверки по запросу Надзорным органам.

Контрольные проверки будут проводиться либо Уполномоченными по защите данных, либо отделом внутреннего аудита Fresenius, либо внешними аудиторами в сотрудничестве с Уполномоченными по защите данных соответствующего подразделения с учетом любых конфликтов интересов путем исключения случаев, когда аудитор проверяет свой собственный участок работы.

## **10.7 Обновление ОКП**

Законодательство о защите данных, а также средства, объем и цели Обработки данных в целом постоянно совершенствуются. Стороны будут анализировать их по мере их появления и оценивать необходимость внесения изменений в ОКП. Поэтому Fresenius оставляет за собой право вносить поправки в ОКП, включая, среди прочего, добавление новых Сторон к ОКП или удаление Сторон из ОКП.

Любые изменения в ОКП, которые существенно повлияют на уровень защиты данных, предлагаемый ОКП, или на сами ОКП, включая административные изменения, если они влияют на ОКП, будут незамедлительно доводиться до сведения каждой Стороны и Надзорного органа в Гессене, Германия (Руководит работой по ОКП). О любых других несущественных поправках к ОКП будет сообщаться Надзорному органу в Гессене, Германия, ежегодно, включая краткое объяснение причин, оправдывающих внесение поправки; Стороны будут уведомлены о таких изменениях максимально оперативно, в любом случае не менее чем за два (2) месяца до вступления в силу поправок или изменений в ОКП. Все поправки и изменения в ОКП будут публиковаться ежегодно. Во избежание сомнений: Надзорный орган в Гессене, Германия, имеет право передавать любой из этих отчетов другим Надзорным органам.

Уполномоченные по защите данных FSE и FK AG совместно ведут обновляемый журнал регистрации, который включает (i) сведения обо всех Сторонах, связанных обязательствами по ОКП, и (ii) учет всех обновлений ОКП. Они также предоставляют возможность Надзорным

органам или Физическим лицам получать по запросу доступ к информации журнала регистрации.

### 11 Управление выходом

В случае, если Сторона перестает соблюдать ОКП (т. е. путем прекращения действия соответствующего внутригруппового соглашения), такая Сторона должна либо (i) незамедлительно и соответственно вернуть все Персональные данные любым Сторонам, передавшим Персональные данные выходящей Стороне в течение периода участия последней в ОКП, или (ii), в соответствии с местными правилами хранения данных, уничтожить все такие Персональные данные и письменно подтвердить Передающим сторонам, что такие Персональные данные были уничтожены, или (iii) иным образом обеспечить достаточные меры защиты в отношении таких Персональных данных в рамках значения статьи 44 и последующих статей ОРЗД (например, путем заключения стандартных договорных положений, принятых Комиссией ЕС). Если выходящая Сторона не может обеспечить такие достаточные меры защиты, выходящая Сторона может только продолжать Обработку таких Персональных данных в будущем и в порядке применения исключения в соответствии со статьей 49 ОРЗД (т.е. только для таких целей, на которые распространяется соответствующее исключение).

### 12 Список использованных источников

н/д

### 13 История изменений документа

Версия	Причина изменения и описание изменения	Автор	Дата
1	Final FDPB	DPO	15.07.2022

### Приложение 1: Список сторон, связанных обязательствами по ОКП

№	Название и описание хозяйственного подразделения Fresenius	Страна учреждения
1	Fresenius Kabi S.A	Аргентина
2	Nutri Home S.A	Аргентина
3	Fresenius Kabi Australia Pty Ltd.	Австралия
4	Fresenius Kabi Austria GmbH	Австрия
5	Fresenius Kabi N.V.	Бельгия
6	Gan Rio Apoio Nutricional - Ganutre Ltda.	Бразилия
7	Fresenius Kabi Brasil Ltda.	Бразилия
8	Fresenius HemoCare Brasil Ltda.	Бразилия
9	Fresenius Kabi Bulgaria EOOD	Болгария
10	Fresenius Kabi Canada Ltd.	Канада

11	Calea Ltd.	Канада
12	Calea Vancouver Inc.	Канада
13	Calea Pharmacy Ltd.	Канада
14	Fenwal International Inc., Cayman Islands	Большой Кайман
15	Fenwal International Inc., Dominican Republic branch	Доминиканская Республика
16	Fenwal International Inc., Puerto Rico branch	Пуэрто-Рико
17	Fresenius Kabi Chile Ltda.	Чили
18	Recetario Magistral Endovenoso S. A.	Чили
19	Laboratorio Sanderson S. A.	Чили
20	Beijing Fresenius Kabi Pharmaceutical Co., Ltd.	Китай
21	Fresenius Kabi (Beijing) Pharmaceutical Distribution Co. Ltd.	Китай
22	Fresenius Kabi (China) Co. Ltd.	Китай
23	Fresenius Kabi (Guangzhou) Co. Ltd.	Китай
24	Fresenius Kabi (Nanchang) Co., Ltd.	Китай
25	Fresenius Kabi Sino-Swed Pharmaceutical Corp. Ltd.	Китай
26	Fresenius Kabi Colombia S.A.S.	Колумбия
27	Fresenius Kabi d.o.o.	Хорватия
28	Fresenius Kabi Horatev CZ s.r.o.	Чешская Республика
29	Fresenius Kabi s.r.o.	Чешская Республика
30	Fresenius Kabi S.A.	Эквадор
31	Fresenius Kabi Scientific Office - Egypt	Египет
32	Fenwal France S.A.S.	Франция
33	Fresenius Kabi France S.A.S.	Франция
34	Fresenius Kabi Groupe France S.A.S.	Франция
35	Fresenius Vial S.A.S.	Франция
36	Fresenius HemoCare GmbH	Германия
37	Fresenius Kabi AG	Германия
38	Fresenius Kabi Deutschland GmbH	Германия
39	Fresenius Kabi Logistik GmbH	Германия

40	medi1one Medical GmbH	Германия
41	MC Medizintechnik GmbH	Германия
42	Fresenius Kabi Ltd.	Великобритания
43	Calea U.K. Ltd.	Великобритания
44	Fresenius Kabi Hellas AEE	Греция
45	Fresenius Kabi Asia Pacific Ltd.	Гонконг
46	Fresenius Kabi Hongkong Ltd.	Гонконг
47	Fresenius Kabi Hungary Kft.	Венгрия
48	Fresenius Kabi India Pvt. Ltd.	Индия
49	Fresenius Kabi Oncology Limited	Индия
50	PT. Fresenius Kabi Indonesia	Индонезия
51	PT. Fresenius Kabi Combiphar	Индонезия
52	Fresenius Kabi Ltd, Ireland branch.	Ирландия
53	Fresenius HemoCare Italia S.r.l.	Италия
54	Fresenius Kabi Italia S.r.l.	Италия
55	Fresenius Kabi iPSUM S.r.l.	Италия
56	Fresenius Kabi Japan K.K.	Япония
57	Fresenius Kabi Korea Ltd.	Южная Корея
58	Fresenius Kabi Baltics UAB	Литва
59	Fresenius Kabi Malaysia Sdn Bhd	Малайзия
60	Fresenius Kabi México, S.A. de C.V.	Мексика
61	Fresenius Kabi Nederland B.V.	Нидерланды
62	Fresenius HemoCare Netherlands B.V.	Нидерланды
63	EnzyPep B.V.	Нидерланды
64	Fresenius Kabi NZ Ltd.	Новая Зеландия
65	Fresenius Kabi Norge A/S	Норвегия
66	Fresenius Kabi Pakistan (Private) Limited	Пакистан
67	Fresenius Kabi Peru SA	Перу
68	Fresenius Kabi Philippines Inc.	Филиппины
69	Fresenius Kabi Polska Sp. z o.o.	Польша
70	Fresenius Kabi Business Services Sp.z.o.o.	Польша
71	DOM Medica Sp. z o.o.	Польша
72	Clinico Medical Sp. z o.o.	Польша

73	Fresenius Kabi Pharma Portugal Lda.	Португалия
74	Labesfal - Laboratórios Almiro, S.A.	Португалия
75	Fresenius Kabi Romania S.R.L.	Румыния
76	Fresenius Kabi LLC	Российская Федерация
77	Fresenius Kabi d.o.o. Beograd	Сербия
78	Fresenius Kabi (Singapore) Pte Ltd.	Сингапур

79	Fresenius Kabi South Africa (Pty) Ltd.	Южная Африка
80	Fresenius Kabi Manufacturing SA (Pty) Ltd.	Южная Африка
81	Fresenius Kabi Grupo España S.L.	Испания
82	Fresenius Kabi España S.A.U.	Испания
83	Quantium Medical S.L.U.	Испания
84	Fresenius Kabi AB, Sweden	Швеция
85	Fresenius Kabi AB, Finish branch	Финляндия
86	Fresenius Kabi AB, Denmark branch	Дания
87	Fresenius Kabi (Schweiz) AG	Швейцария
88	Fresenius Kabi SwissBioSim GmbH	Швейцария
89	FresuCare AG	Швейцария
90	Fresenius Kabi Taiwan Ltd.	Тайвань
91	Fresenius Kabi (Thailand) Ltd.	Таиланд
92	Fresenius Kabi Tunisia S.a.r.l.	Тунис
93	Fresenius Kabi İlaç San. ve Tic. Ltd. Şti.	Турция
94	Fresenius Kabi Middle East FZ-LLC	Объединенные Арабские Эмираты
95	Fresenius Kabi Latin America Exports S.A	Уругвай
96	Fresenius Kabi, LLC	Соединенные Штаты
97	Fresenius Kabi USA, LLC	Соединенные Штаты
98	Fenwal Inc.	Соединенные Штаты
99	Fresenius Kabi Vietnam Joint Stock Company	Вьетнам
100	Representative office of Fresenius Kabi Asia Pacific Limited	Вьетнам
101	Fresenius SE & Co. KGaA	Германия
102	Fresenius Digital Technology GmbH	Германия
103	Fresenius Versicherungsvermittlungsgesellschaft mbH	Германия

104	Fresenius Management SE	Германия
105	Hyginus Publisher GmbH	Германия
106	Fresenius Digital Technology Polska sp. z o.o	Польша
107	Fresenius Netcare Beijing Consulting Co.,Ltd	Китай
108	Fresenius Digital Technology India Private Limited	Индия
109	Fresenius Immobilien-Verwaltungs-GmbH	Германия
110	FPS Immobilien Verwaltungs GmbH	Германия
111	Fresenius ProServe GmbH	Германия
112	Fresenius Finance Ireland PLC	Ирландия
113	Fresenius Finance Ireland II PLC	Ирландия
114	Fresenius Finance Holdings Ltd	Ирландия
115	Fresenius Kabi Business Services Manila Inc	Филиппины
116	GH Genhelix, S.A. (Unipersonal),	Испания
117	Mabxience Research, S.L. (Unipersonal),	Испания
118	Mabxience, S.A.U.	Аргентина
119	Mabxience, S.A	Швейцария
120	Mabxience Holding, S.L.,	Испания



**Приложение 2: Характер передаваемых Персональных данных**

Следующие Персональные данные подлежат Передаче в соответствии с ОКП для следующих целей:

**Отдел кадров**

Следующие Персональные данные руководителей, Сотрудников и претендентов на работу любой Стороны могут быть переданы другим Сторонам для целей, описанных в настоящем Приложении:

Цель	Категории данных
<ul style="list-style-type: none"> <li>• Управление трудовыми отношениями</li> <li>• Управление и обслуживание в сфере ИТ и коммуникаций для сотрудников</li> <li>• Внешние коммуникации и вебсайт</li> <li>• Управление рабочим процессом и производительностью, санкции</li> <li>• Управление в сфере знаний и обучения</li> <li>• Зарплата</li> <li>• управление/зарплата ведомость/ льготы/пенсии</li> <li>• Планирование кадров и ресурсов</li> <li>• Подбор, продвижение по службе и обеспечение кадрами</li> <li>• Внутренние коммуникации, внутренняя сеть</li> <li>• Слияния и поглощения</li> <li>• Обеспечение нормативно-правового соответствия, нормативные требования</li> </ul>	<ul style="list-style-type: none"> <li>• Идентификационные данные и личные характеристики (имя, возраст, пол, национальность, номер государственного удостоверения личности, фотография и контактные данные)</li> <li>• Условия трудоустройства, квалификация, должностная инструкция</li> <li>• Финансовые данные (заработная плата, страхование, налоги, пенсии и льготы)</li> <li>• Планирование и производительность работы (рабочий процесс, проекты и задания; отработанное время; оценка; санкции)</li> <li>• Деятельность в профсоюзах или трудовом совете</li> <li>• Состояние здоровья</li> <li>• Использование коммуникаций и ИТ</li> <li>• Расследования несоответствия нормативно-правовым требованиям</li> <li>• Информация о юридических спорах</li> <li>• Справки из полиции (при условии, что в них нет записей)</li> </ul>

**Клиент**

Следующие Персональные данные клиентов и контактных лиц клиентов любой Стороны могут быть переданы другим Сторонам в целях, описанных ниже:

Цель	Категории данных
------	------------------

## Обязательные корпоративные правила (ОКП)

- |   |   |
|---|---|
| <ul style="list-style-type: none"> <li>• Выполнение договоров/производство, поставка и доставка продукции и услуг/обращение с претензиями</li> <li>• Управление взаимоотношениями с клиентами</li> <li>• Финансы/выставление счетов/сбор платежей/бухгалтерский учет</li> <li>• Маркетинг/отношения с клиентами и управление клиентскими счетами</li> <li>• Слияния и поглощения</li> <li>• Обеспечение нормативно-правового соответствия и выполнение нормативных требований, таких как комплексная проверка деловых партнеров, отслеживание санкционного списка, борьба с отмыванием денег, защищенная цепочка поставок, таможенное и экспортное законодательство, отслеживание продуктов, рейтинг кредитного риска.</li> </ul> | <ul style="list-style-type: none"> <li>• Имя, род деятельности, должность и контактные данные</li> <li>• Бизнес клиента</li> <li>• Деловые операции и отношения с клиентом</li> <li>• Финансовые данные (банковские операции и выставление счетов)</li> <li>• Использование коммуникаций и ИТ</li> <li>• Подробности, касающиеся публичной отчетности, торговых реестров и профессиональных советов.</li> </ul> |
|---|---|

### Пациенты

Следующие Персональные данные пациентов и вспомогательных лиц (например, лиц, осуществляющих уход) любой Стороны могут быть переданы другим Сторонам для целей, описанных ниже:

Цель	Категории данных
<ul style="list-style-type: none"> <li>• Выполнение договоров/производство, поставка и доставка продукции и услуг/ работа с претензиями</li> <li>• Управление отношениями с пациентами</li> <li>• Маркетинг/взаимоотношения с пациентами и управление клиентскими счетами</li> <li>• Финансы/выставление счетов/сбор платежей/бухгалтерский учет</li> </ul>	<ul style="list-style-type: none"> <li>• Идентификационные данные и личные характеристики (имя, возраст, пол, национальность и контактные данные)</li> <li>• Медицинские записи и состояние здоровья</li> <li>• Лечение и отношения с пациентом</li> <li>• Финансовые данные (банковские операции и выставление счетов)</li> <li>• Коммуникация и использование ИТ</li> </ul>
<ul style="list-style-type: none"> <li>• Обеспечение нормативно-правового соответствия и выполнение нормативных требований</li> <li>• Слияния и поглощения</li> <li>• Клинические испытания, исследования и разработки</li> <li>• Экстренная помощь/нежелательные явления и мониторинг безопасности медицинских изделий</li> </ul>	

### Поставщик

## Обязательные корпоративные правила (ОКП)

Следующие Персональные данные поставщика и контактных лиц поставщиков любой Стороны могут быть переданы другим Сторонам в целях, описанных ниже:

Цель	Категории данных
<ul style="list-style-type: none"> <li>• Маркетинг/управление взаимоотношениями с поставщиками</li> <li>• Администрирование отношений с поставщиками</li> <li>• Выполнение договоров/производство, поставка и доставка продукции и услуг/обращение с претензиями</li> <li>• Финансы/выставление счетов/бухгалтерский учет</li> <li>• Слияния и поглощения</li> <li>• Обеспечение нормативно-правового соответствия и выполнение нормативных требований, таких как комплексная проверка деловых партнеров, отслеживание санкционного списка, борьба с отмыванием денег, защищенная цепочка поставок, таможенное и экспортное законодательство, отслеживание продуктов, рейтинг кредитного риска.</li> </ul>	<ul style="list-style-type: none"> <li>• Имя, род деятельности, должность и контактные данные</li> <li>• Бизнес поставщика</li> <li>• Деловые операции и отношения с поставщиком</li> <li>• Финансовые данные (банковские операции и выставление счетов)</li> <li>• Использование коммуникаций и ИТ</li> <li>• Подробности, касающиеся публичной отчетности, торговых реестров и профессиональных советов.</li> </ul>

### Другие цели

Следующие Персональные данные других Физических лиц (например, контактных лиц для экстренных случаев, контактных лиц прессы) могут быть переданы другим Сторонам для целей, описанных ниже:

Цель	Категории данных
<ul style="list-style-type: none"> <li>• Разрешение экстренных ситуаций</li> <li>• ИТ</li> <li>• Безопасность</li> <li>• Регулярное администрирование почты, мониторинг</li> </ul>	<ul style="list-style-type: none"> <li>• Имя и контактные данные</li> <li>• Подключение к Fresenius или Физическому лицу Fresenius</li> <li>• Другая информация, необходимая для этой цели.</li> </ul>