

Переход к глобальной политике

Глобальная политика конфиденциальности данных

Владелец документа	Анна Ромберг
Версия	v3
Принято Советом директоров	26 апреля 2023 года

1. Резюме

Целью настоящей Глобальной политики конфиденциальности данных (**“Глобальная политика”**) является установление основных требований к конфиденциальности данных и предоставление руководству Getinge, сотрудникам и консультантам рекомендаций в их повседневной работе, связанной с обработкой персональных данных.

Getinge обязуется обрабатывать персональные данные в соответствии с применимыми законами и нормативными актами о защите данных. Конфиденциальность всегда должна быть главным приоритетом в нашей повседневной деятельности.

Настоящая Глобальная политика распространяется на всех сотрудников, директоров и деловых партнеров, действующих от имени Getinge.

2. Определения

В настоящей Глобальной политике следующие термины имеют следующее значение:

Контроллер данных	Юридическое лицо, которое самостоятельно или совместно с другими юридическими лицами определяет цели и средства обработки персональных данных.
Обработчик данных	Юридическое лицо, которое обрабатывает персональные данные от имени Контролера данных.
Оценка воздействия на защиту данных	Систематический процесс оценки проекта, процесса или решения с точки зрения его влияния на защиту данных.
Законы о защите данных	Любые применимые законы и нормативные акты о защите данных, включая, но не ограничиваясь, GDPR.
Субъект данных	Физическое лицо, к которому относятся Персональные данные.

GDPR

Постановление (ЕС) 2016/679 Европейского парламента и Совета от 27 апреля 2016 года о защите физических лиц в отношении обработки персональных данных и о свободном перемещении таких данных и отмене Директивы 95/46/ЕС.

личные данные

Любая информация, относящаяся к Субъекту данных. Субъект данных - это тот, кого можно идентифицировать, прямо или косвенно, используя имя, идентификационный номер, данные о местоположении, онлайн-идентификатор или факторы, специфичные для физической, физиологической, генетической, ментальной, экономической, культурной или социальной идентичности этого физического лица. Персональные данные также включают контактные данные сотрудников, такие как рабочие адреса электронной почты и контактные лица.

Утечка персональных данных

Нарушение безопасности, приводящее к случайному или незаконному уничтожению, потере, изменению, несанкционированному раскрытию или доступу к передаваемым, хранящимся или иным образом обрабатываемым персональным данным.

Обработка персональных данных

Любая операция или набор операций, которые выполняются с персональными данными или с наборами персональных данных, независимо от того, автоматизированы они или нет, такие как сбор, запись, организация, структурирование, хранение, адаптация или чередование, извлечение, консультирование, раскрытие использования путем передачи, распространения или иного предоставления доступа, согласование или комбинация, ограничение, стирание или уничтожение. Обработка также включает в себя просмотр персональных данных.

Особые категории персональных данных-

Все персональные данные, прямо или косвенно указывающие на расовое или этническое происхождение живого физического лица, политические взгляды, философские или религиозные убеждения,

сексуальную ориентацию, членство в профсоюзах и деятельность, генетические или биометрические данные, а также данные, касающиеся здоровья или сексуальной жизни.

Надзорный орган

Независимый государственный орган, ответственный за контроль за соблюдением законов о защите данных.

3. Сфера охвата и цель

Настоящая Глобальная политика действительна для всех компаний Getinge, ее дочерних компаний и совместных операций (совместно именуемых **“Getinge”**) и распространяется на всех наших сотрудников, а также консультантов и персонал агентств, которые работают в помещениях Getinge или под руководством Getinge (все они именуются в настоящей Глобальной политике **“сотрудники”**). Общее правило заключается в том, что настоящая Глобальная политика применяется ко всей обработке персональных данных в рамках Getinge. Исключения применяются только в случаях, изложенных в настоящей Глобальной политике.

Цель этой глобальной политики состоит в том, чтобы обеспечить:

- a) Общие знания о персональных данных и применимых законах о защите данных
- b) Руководство по юридическим требованиям, которые имеют первостепенное значение для Getinge
- c) Требования к получению информации при обработке персональных данных
- d) Инструкции, которым необходимо следовать при обработке персональных данных Getinge

В соответствии с этой Глобальной политикой мы обязуемся защищать персональные данные в соответствии с законами о защите данных.

4. Область применения

Конкретика в отношении применимости

Эта глобальная политика применяется к:

- a) Обработка персональных данных в бизнес-процессах
- b) ИТ-функции, решения или сервисы, используемые для обработки персональных данных
- c) Такие инструменты, как Outlook, PowerPoint, Word и Excel
- d) Ситуации, когда Getinge предоставляет продукты или услуги, которые будут включать обработку персональных данных от имени третьей стороны, например, ИТ-решения, предоставляемые больницам

- е) Все остальные ситуации, когда Getinge является либо Контролером данных, Обработчиком данных и/или Совместным контролером, как описано в настоящей Глобальной политике

Для конкретных операций могут потребоваться другие требования, отличные от тех, которые указаны в настоящей Глобальной политике, например требования, касающиеся ИТ-безопасности. В дополнение к этой Глобальной политике могут существовать дополнительные инструкции и руководящие принципы по обработке персональных данных, применимые к конкретным командам Getinge.

Применимые законы, местные требования и отклонения

Настоящая Глобальная политика основана на европейских законах и нормативных актах по защите данных, но актуальна и применима ко всей обработке персональных данных Getinge также за пределами ЕС/ЕЭЗ. Причинами, по которым европейские законы и нормативные акты о защите данных применимы к такой обработке, могут быть, например, следующие:

- а) Обработка относится к процедурам, системам, распорядку дня или решениям, принятым штаб-квартирой Getinge, которая базируется в ЕС/ЕЭЗ
- б) Обработка относится к товарам и услугам, предлагаемым субъектам данных в пределах ЕС/ЕЭЗ, или мониторингу их поведения
- с) Организация за пределами ЕС/ЕЭЗ считается созданной в ЕС/ЕЭЗ из-за, например, наличия сотрудников в ЕС/ЕЭЗ

Если местные законы и нормативные акты о защите данных предъявляют требования, отличные или более строгие, чем те, которые установлены настоящей Глобальной политикой, Getinge обязана соблюдать такие законы и нормативные акты. Если законы и/или нормативные акты вступают в противоречие с настоящей Глобальной политикой, преимущественную силу имеют более строгие требования. Для получения дальнейших указаний, пожалуйста, свяжитесь с отделом защиты персональных данных.

Анонимизированные и псевдонимизированные данные

Настоящая Глобальная политика не распространяется на информацию, которая является *полностью* анонимной, т.е. информацию, которая не может быть связана с идентифицируемым физическим лицом. Благодаря техническим решениям, доступным на современном рынке, существует множество различных способов идентификации людей с помощью правильных технических инструментов. Обратите внимание, что анонимизация может оказаться сложной задачей для достижения на практике.

Эта глобальная политика действительно применяется к информации, которая подверглась так называемой псевдонимизации, то есть к информации, которая может быть привязана к конкретному лицу с использованием другого набора информации (например, «ключа»). Псевдонимизированные данные по-прежнему считаются персональными данными.

обратите внимание!

Персональные данные не считаются анонимизированными, если данные, хранящиеся в компании Getinge, в сочетании с другими данными, хранящимися в другой компании Getinge или третьей стороне, могут быть связаны с физическим лицом. Например, как статические, так и динамические IP-адреса считаются персональными данными, поскольку IP-номер может быть связан с физическими лицами, если он объединен с

информацией, хранящейся у интернет-оператора. Не имеет значения, что Getinge не может получить доступ к информации, хранящейся у третьей стороны, т.е. она по-прежнему считается персональными данными.

5. Ответственность за соблюдение требований

Команда по защите данных

Организация Getinge по защите данных и команда по защите данных описаны в Директиве по управлению конфиденциальностью данных. Команда по защите данных должна обладать необходимыми экспертными знаниями в области защиты данных.

Команда по защите данных должна рассматриваться как партнер по обсуждению в рамках Getinge, и мнению команды по защите данных должно придаваться должное значение в вопросах конфиденциальности данных.

Смотрите далее: Директива по управлению конфиденциальностью данных

Ответственность компаний-получателей

Конечная ответственность каждой компании Getinge заключается в соблюдении законов, нормативных актов, внутренних решений Getinge, процессов и процедур, изложенным в настоящей Глобальной политике. Смотрите также раздел 19, касающийся ролей и обязанностей.

Отчетность о рисках

Getinge будет стремиться полностью соблюдать все законы о защите данных и активно выявлять и исправлять деловую практику, которая приводит или потенциально может привести к нарушениям. Каждого сотрудника поощряют и ожидают, что он будет сообщать о любых инцидентах или подозрениях в несоблюдении требований с гарантией того, что не будет никаких ответных мер или других негативных последствий для лиц, действующих добросовестно. Ожидается, что сотрудники будут сообщать о рисках для конфиденциальности данных и/или подозрениях в несоблюдении требований в Отдел по защите данных. Вопросы также всегда могут быть подняты в соответствии с разделом 18.

6. Общие требования, предъявляемые к компаниям Getinge при обработке персональных данных в качестве контролера или совместного контролера

Контроллер

Когда компания Getinge обрабатывает персональные данные, она может делать это по собственной инициативе, определяя, почему и как будут обрабатываться Персональные данные. Если компания Getinge определяет средства (как) и цели (почему) обработки персональных данных, она именуется Контролером данных.

пример

Если Getinge собирает персональные данные о своих сотрудниках для целей выплаты заработной платы каждый месяц, Getinge определяет цели и средства обработки и, следовательно, считается контролером обработки персональных данных.

Совместный контроллер

При определенных обстоятельствах два или более контролера данных могут совместно определять цели (почему) и средства (как) обработки персональных данных. Например, компания Getinge может совместно выполнять роль контролера данных с одной или несколькими внутренними и/или внешними организациями. Это называется совместным управлением.

При наличии отношений с совместным контролером существует юридическое требование о заключении соглашения о совместном контролере, определяющего соответствующие обязанности контролеров данных. Компания Getinge должна обеспечить использование соответствующего шаблона, доступного во внутренней сети.

пример

Если компания Getinge проводит исследование совместно с больницей, в ходе которого компания Getinge и больница совместно определяют, почему и как будут обрабатываться персональные данные в рамках проекта, компания Getinge и больница могут рассматриваться как совместные контролеры, и в таком случае им потребуется заключить соглашение о совместном контролере.

Основные требования к сбору и обработке персональных данных

Персональные данные могут обрабатываться только в определенных, недвусмысленных и законных целях. Для того чтобы цели считались законными, планируемая обработка должна осуществляться независимо от того, дал ли Субъект данных согласие на обработку:

- a) Преследуют законную деловую цель и не могут нарушать какие-либо законы о защите данных или другие законодательные акты;
- b) Быть пропорциональным и необходимым для достижения целей;
- c) Не должны использоваться способами, которые оказывают неоправданное негативное воздействие на субъектов данных; и
- d) Обрабатывайте персональные данные Субъектов данных только таким образом, которого Субъекты данных разумно ожидали бы.

Любая обработка персональных данных должна быть необходима для достижения цели обработки, и Субъекты данных не должны быть введены в заблуждение относительно целей или объема обработки их персональных данных. Персональные данные не могут обрабатываться каким-либо образом, несовместимым с целями, о которых был уведомлен Субъект данных. Кроме того, персональные данные, обрабатываемые компаниями Getinge, должны быть точными и, при необходимости, обновляться.

Правовая основа для обработки персональных данных

Общие сведения о правовой основе

Getinge может обрабатывать персональные данные только в том случае, если применяется хотя бы одно из следующих условий:

- a) **Согласие.** Субъект данных предоставил предварительное согласие на обработку в указанных целях. Смотрите ниже в этом разделе 6 информацию о согласии и отзыве согласия.
- b) **Юридическое обязательство.** Getinge должна обрабатывать персональные данные для выполнения юридических обязательств, которым подчиняется Getinge (например, для предоставления информации о налоговых доходах в налоговые органы).
- c) **Исполнение контракта.** Обработка персональных данных необходима Getinge для выполнения своих обязательств по контракту, который она заключила с Субъектом данных (например, сохранение реквизитов банковского счета для выплаты заработной платы по трудовому договору).
- d) **Законный интерес Гетинга.** Getinge может обрабатывать персональные данные в законных целях в рамках своей деятельности (например, вести базу данных информации о своих клиентах или деловых партнерах или собирать имена и номера телефонов экстренных контактов для своих сотрудников), за исключением случаев, когда такие интересы перекрываются интересами или основными правами и свободами данных Субъект. При применении этой правовой основы необходимо определить конкретный интерес, о котором идет речь, и проинформировать об этом Субъекта данных.
- e) **Другой.** Существуют и другие редкие основания, по которым персональные данные могут обрабатываться, а именно защита жизненно важных интересов субъекта данных или выполнение задач в общественных интересах.

Согласие и отзыв согласия

Согласие должно использоваться компаниями Getinge только в тех случаях, когда не может быть использовано никакое другое правовое основание. Если согласие применяется в качестве юридического основания, компания Getinge должна быть в состоянии продемонстрировать, что Субъект данных дал согласие на обработку персональных данных и что такое согласие является действительным. Заранее поставленные галочки, молчание или бездействие никогда не являются согласием. При необходимости следует получить отдельные согласия для различных целей обработки.

Согласие должно быть:

- a) Дается без соблюдения других условий;
- b) Информированный (смотрите ниже в этом разделе информацию для субъектов данных);
- c) Предоставлено добровольно (субъект данных не должен испытывать давления с целью предоставления согласия); и
- d) Конкретный и недвусмысленный (субъект данных должен быть осведомлен о сфере действия согласия).

Согласие должно быть дано в письменной форме или в электронном виде. Должно быть четко указано, соглашается ли Субъект данных с предлагаемой обработкой персональных данных. Согласие не может быть получено молчанием или бездействием.

Субъект данных может отозвать предоставленное согласие в любое время. При отзыве согласия соответствующая компания Getinge прекращает обработку персональных данных о

Субъекте данных в той мере, в какой обработка основана на согласии. Это означает, что все персональные данные о физическом лице, отозвавшем согласие, должны быть удалены или обезличены, включая персональные данные в любых резервных копиях.

Дополнительные требования к обработке особых категорий персональных данных

Особые категории персональных данных, часто называемые “Конфиденциальными персональными данными”, пользуются особой защитой и не должны обрабатываться компанией Getinge, за исключением особых обстоятельств.

Обработка особых категорий персональных данных может осуществляться только при наличии законных оснований для обработки, как описано выше в настоящем разделе 6. Кроме того, такие данные могут быть обработаны только при соблюдении хотя бы одного из следующих условий:

- а) Субъект данных предоставил явное согласие на обработку в указанных целях;
- б) Обработка необходима для целей выполнения обязательств и осуществления прав Контролера данных или Субъекта данных в области трудового законодательства в той мере, в какой это разрешено национальными законами или коллективными соглашениями;
- с) Обработка необходима для предъявления, осуществления или защиты юридического иска; или
- д) Обработка необходима в целях профилактики или медицины труда, для оценки трудоспособности работника, постановки медицинского диагноза, оказания медицинской помощи или лечения.

Getinge, как правило, следует избегать обработки особых категорий персональных данных и может делать это только в том случае, если применяется одно или несколько из вышеперечисленных условий. Также могут применяться местные исключения.

обратите внимание!

Явное согласие содержит требования к обычному согласию, как описано выше в этом разделе 6, касающемся согласия и отзыва согласия. Кроме того, физическому лицу должна быть четко предоставлена возможность согласиться или не согласиться с предлагаемой обработкой персональных данных.

Персональные данные в связи с уголовными преступлениями и обвинительными приговорами

Getinge не будет обрабатывать никакие персональные данные, относящиеся к уголовным преступлениям или обвинительным приговорам, включая подозрения, за исключением случаев, когда это разрешено или требуется применимыми законами и нормативными актами. Обратите внимание, что существует общий запрет на обработку персональных данных такого типа. Однако исключения могут быть предусмотрены в национальных законах и нормативных актах.

Различные отделы Getinge могут предъявлять требования к обработке персональных данных, относящихся к уголовным преступлениям, обвинительным приговорам или связанным с ними подозрениям. Например, в контексте расследований и/или должной осмотрительности существуют требования (если они подкреплены применимым

законодательством и нормативными актами) к юридическому отделу, отделу комплаенса и управления по установлению фактов, проверке биографических данных компаний и/или персонала, занимающего соответствующие должности.

обратите внимание!

Перед обработкой любых персональных данных, касающихся судимостей, уголовных правонарушений, обвинительных приговоров или связанных с ними подозрений, всегда следует проконсультироваться со службой защиты данных.

Информация для субъектов данных

Getinge направляет Субъектам данных письменное уведомление с информацией о:

- a) Имя и контактные данные юридического лица, которое является контролером данных;
- b) Типы обрабатываемых персональных данных и связанные с ними цели обработки;
- c) Правовая основа обработки;
- d) Как долго будут храниться персональные данные;
- e) Получатели или категории получателей персональных данных;
- f) Информация о правах субъекта данных в соответствии с разделом 8 ниже; и
- g) Если применимо:
 - i. контактные данные ответственного сотрудника по защите данных;
 - ii. откуда были получены персональные данные;
 - iii. последствия, если Субъект данных не предоставит свои персональные данные;
 - iv. Намерения Getinge передать персональные данные за пределы ЕС/ЕЭЗ в соответствии с разделом 9 ниже; и
 - v. Информация о профилировании.

Команда по защите данных предоставляет шаблоны уведомлений о конфиденциальности, которые всегда должны использоваться, когда компании Getinge необходимо проинформировать субъектов данных об обработке персональных данных. Шаблоны содержат дополнительные инструкции по информации, которая должна быть предоставлена субъектам данных.

Каждая компания Getinge несет ответственность за обеспечение и демонстрацию того, что ее уведомления о конфиденциальности являются достаточными и полными и что она соответствует законам о защите данных. Кроме того, компании Getinge при необходимости переводят уведомления о конфиденциальности на местный язык.

Что касается сотрудников, информация об обработке персональных данных обычно предоставляется в Уведомлении о конфиденциальности сотрудников, которое сотрудники получают вместе с трудовым договором. Каждая компания Getinge должна обеспечить, чтобы ее Уведомление о конфиденциальности сотрудников было легкодоступным для сотрудников и актуальным, а также содержало достаточную информацию о том, как компания обрабатывает персональные данные сотрудников.

Измененные цели обработки персональных данных

Прежде чем изменить цели обработки персональных данных, компания Getinge обязана:

- a) Оцените законность обработки персональных данных и задокументируйте оценку в соответствии с разделом 7 ниже;

- b) Предоставить Субъекту данных письменную информацию, описывающую изменения в целях обработки; и
- c) Если обработка основана на согласии, получите новое согласие от Субъекта данных.

Профилирование и автоматизированное принятие решений

Общие сведения о профилировании

Профилирование подразумевает любую форму автоматизированной обработки персональных данных, предполагающую намерение оценить личные аспекты, относящиеся к Субъекту данных, или предсказать или проанализировать эффективность работы этого субъекта данных, экономическую ситуацию, местоположение, здоровье, личные предпочтения, интересы, надежность или поведение, поведение водителя, поведение клиента, местоположение или передвижение.

Профилирование часто используется для составления прогнозов относительно отдельных лиц на основе данных из различных источников и статистических выводов. Целью обработки может быть анализ характеристик или моделей поведения Субъекта данных с целью отнесения его к определенной группе или категории. Это позволяет Контролеру данных делать прогнозы, например, относительно интересов субъекта данных, способности выполнить задачу или вероятного поведения.

примеры

Профилирование может, например, состоять из анализа поведения пользователя на веб-сайтах с помощью идентификаторов файлов cookie или IP-адресов с целью отправки персонализированной рекламы, касающейся конкретных продуктов или услуг. Другой пример профилирования касается анализа предыдущих покупок с целью прогнозирования будущих покупок. Таким образом, профилирование - это метод, обычно используемый в связи с прямым маркетингом и социальными сетями, но также может быть использован для других видов обработки, таких как научные исследования.

Решения, основанные на профилировании

Решение, принятое компанией Getinge на основе профилирования, допускается только в том случае, если:

- a) это абсолютно необходимо для заключения или исполнения соглашения между Субъектом данных и Контролером данных (это исключение следует толковать узко).;
- b) это прямо разрешено законом, в том числе в целях мониторинга и предотвращения мошенничества и уклонения от уплаты налогов, проводимых в соответствии с правилами, стандартами и рекомендациями учреждений или национальных надзорных органов, а также для обеспечения безопасности и надежности услуг, предоставляемых Getinge; или
- c) Субъект данных предоставил явное согласие.

Требования

Участвуя в профилировании, компании Getinge должны обеспечить следующее:

- a) Обработывайте только необходимые персональные данные для достижения поставленной цели;
- b) Предоставлять субъектам данных достаточную информацию о профилировании в соответствии с разделом 6. Если профилирование касается автоматизированного принятия решений, субъекты данных имеют право получить объяснение по поводу принятого решения, а также информацию о праве возражать против такого решения;
- c) Используйте адекватные математические или статистические процедуры для составления профиля;
- d) Осуществить соответствующие технические и организационные меры в соответствии с разделом 0; и
- e) Защищайте персональные данные таким образом, который учитывает потенциальные риски, связанные с правами и интересами субъектов данных, и который, в частности, предотвращает дискриминационные последствия в отношении отдельных лиц на основе особых категорий персональных данных или которые приводят к мерам, имеющим такой эффект.

обратите внимание!

Профилирование должно быть предварительно одобрено командой по защите данных до его проведения.

Хранение, сохранность и удаление персональных данных

Компании Getinge должны обеспечить, чтобы персональные данные не обрабатывались дольше, чем:

- a) необходимо в связи с целью (целями) обработки; и
- b) разрешено законами о защите данных.

Компании Getinge должны внедрить processed для обеспечения выполнения требований, изложенных в этом разделе.

обратите внимание!

Некоторые страны (например, Россия и Китай) требуют, чтобы все персональные данные о их гражданах хранились в пределах границ страны. В других странах могут существовать требования к хранению определенных персональных данных на местном уровне, если они обрабатываются для определенных целей (например, Швеция требует, чтобы бухгалтерская информация хранилась в пределах ее границ). Требования к локализации, как правило, не препятствуют Getinge также хранить копию персональных данных в другом месте, если такое хранение необходимо.

7. Оценка и документирование процесса обработки

Запись операций по обработке

Когда того требуют законы о защите данных, компании Getinge несут ответственность за ведение учета операций компаний по обработке данных. Все записи должны храниться в

инструменте соответствия требованиям, выбранном и обрабатываемом командой по защите данных. Дополнительную информацию можно найти на странице внутренней сети, посвященной защите данных.

Требования, изложенные в этом разделе, применяются как в тех случаях, когда компании Getinge выступают в качестве контролеров данных, так и в качестве обработчиков данных.

Оценка законности перед началом новой операции по обработке

Прежде чем осуществлять новую операцию по обработке или вносить изменения в текущую деятельность, компании Getinge должны оценить законность обработки персональных данных и задокументировать результаты оценки. Это также относится к любым текущим операциям по обработке, которые ранее не были оценены и/или задокументированы.

Требования, изложенные в этом разделе, применяются как в тех случаях, когда компании Getinge выступают в качестве контролеров данных, так и в качестве обработчиков данных.

Оценки воздействия на защиту данных

Если обработка персональных данных может привести к высокому риску для прав и свобод субъектов данных, компании Getinge должны до начала такой предполагаемой обработки провести оценку влияния операций по обработке на защиту персональных данных (Оценка воздействия на защиту данных). Оценка воздействия на защиту данных может быть особенно актуальна, когда компании Getinge используют новые технологии и принимают во внимание характер, объем, контекст и цели обработки.

Оценка воздействия на защиту данных всегда должна проводиться командой по защите данных от имени компании Getinge. Компания Getinge обязуется сотрудничать с Отделом защиты персональных данных в ходе оценки, включая, но не ограничиваясь, предоставлением необходимой информации.

8. Права субъекта данных

Обработка запросов субъекта данных

В отношении запросов от субъектов данных применяется следующее:

- a) Все запросы от субъектов персональных данных должны немедленно направляться в Службу защиты персональных данных и обрабатываться ею.
- b) Субъекты данных не могут столкнуться с негативными последствиями при осуществлении прав субъектов данных.
- c) Все запросы субъекта данных должны обрабатываться с соблюдением конфиденциальности.
- d) Компании Getinge должны сотрудничать с Отделом защиты данных, чтобы Отдел защиты данных мог своевременно отвечать на запросы.

Обратите внимание, что права субъекта данных не являются абсолютными и что могут применяться исключения.

Процессы для обработки прав субъектов данных

Компании Getinge отвечают за внедрение процессов, помогающих команде по защите данных в обработке прав субъектов данных на:

- a) Запросите доступ к персональным данным. Это включает в себя право субъектов данных на получение информации об обработке персональных данных, относящихся к соответствующему физическому лицу, и обеспечение права на переносимость данных.
- b) Запросите исправление неточных персональных данных.
- c) Запросите удаление персональных данных.
- d) Возражать в любое время против обработки персональных данных, если обработка основана на законных интересах Getinge, в том числе когда обработка касается профилирования.
- e) Получите ограничение на доступ к персональным данным.

9. Передача персональных данных

Общие сведения о переводах

Персональные данные передаются только для достижения цели (целей) обработки. Передача персональных данных включает в себя не только отправку персональных данных с использованием электронных сообщений, таких как электронная почта, но также включает в себя возможность доступа к персональным данным или их просмотра. Персональные данные считаются переданными, даже если к ним осуществляется лишь временный доступ, просмотр или иная обработка.

пример

Персональные данные передаются, когда компания Getinge во Франции хранит персональные данные в папке, доступ к которой могут получить сотрудники Getinge в Китае (смотрите также в этом разделе 9, касающемся передачи персональных данных из ЕС/ЕЭЗ в страну за пределами ЕС/ЕЭЗ).

Передача персональных данных из ЕС/ЕЭЗ в страну за пределами ЕС/ЕАЭС

Как правило, компании Getinge в ЕС/ЕЭЗ не должны передавать персональные данные за пределы ЕС/ЕЭЗ. Такие переводы могут быть осуществлены только в случае крайней необходимости.

Если передача персональных данных из стран ЕС/ЕЭЗ в страны за пределами ЕС/ЕЭЗ строго необходима, компании Getinge должны обеспечить, чтобы:

- a) такие передачи подлежат надлежащим гарантиям в соответствии с законами о защите данных, включая, но не ограничиваясь ими, передачи, основанные на:
 - i. Решение об адекватности, принятое Европейской комиссией;
 - ii. Стандартные договорные положения ЕС, принятые Европейской комиссией; или
 - iii. Явное согласие.
- b) при необходимости была проведена оценка воздействия переноса.

До передачи Персональных данных субъекты данных имеют право получить информацию о передаче и применимых надлежащих мерах защиты в соответствии с разделом 6.

10. Обмен и раскрытие персональных данных в рамках Getinge

Сотрудники и консультанты Getinge должны передавать и раскрывать персональные данные только тем лицам в Getinge, которые нуждаются в таких данных для выполнения рабочих задач и в тех случаях, когда существует законная деловая цель для обмена или раскрытия таких персональных данных. Персональные данные могут передаваться или раскрываться только в той мере, в какой это необходимо для достижения цели (целей) обработки. Персональные данные не могут быть переданы или разглашены, поскольку их может быть “приятно иметь” получателю.

11. Обработчики данных

Общие положения о положениях в соглашениях

Компании Getinge несут ответственность за включение, при необходимости, положений об обработке персональных данных и/или соглашений об обработке данных в стандартные деловые и трудовые соглашения Getinge.

В случаях, когда существующие соглашения уже действуют, компании Getinge при необходимости обновляют такие соглашения положениями об обработке персональных данных и/или соответствующими соглашениями об обработке данных.

обратите внимание!

Шаблоны соглашений об обработке данных, доступные на странице конфиденциальности данных во внутренней сети, всегда следует использовать в тех случаях, когда требуется соглашение об обработке данных.

Getinge выступает в качестве обработчика данных по отношению к третьим лицам

Если компания Getinge обрабатывает персональные данные от имени третьей стороны (например, клиента), Getinge и третья сторона должны заключить соглашение об обработке данных. Компания Getinge должна обеспечить использование соответствующего шаблона, доступного во внутренней сети.

пример

Getinge в большинстве случаев выступает в качестве обработчика данных в связи с предоставлением наших программных решений больницам. Это тот случай, когда Getinge необходимо получить доступ к персональным данным или иным образом обработать их, когда мы предоставляем поддержку программного обеспечения. В таких ситуациях больница будет выступать в качестве контролера данных.

Заключение контракта с внешним обработчиком данных

Если третья сторона будет обрабатывать персональные данные от имени Getinge (например, поставщик), Getinge и третья сторона должны заключить соглашение об обработке данных. Компания Getinge должна обеспечить использование соответствующего шаблона, доступного во внутренней сети.

пример

Если Getinge приобретает новую ИТ-систему/решение, которое предусматривает, что поставщик ИТ-системы/решения обрабатывает персональные данные от имени Getinge (например, хранит персональные данные и/или получает доступ к персональным данным при оказании поддержки), Getinge и поставщик должны заключить соглашение об обработке данных. В этой ситуации Getinge является контролером данных, а поставщик - обработчиком данных.

Getinge в качестве обработчика данных по отношению к другим компаниям Getinge

Если компания Getinge обрабатывает персональные данные от имени другой компании Getinge, стороны должны заключить внутригрупповое соглашение об обработке данных. Компании/функции Getinge должны обеспечить, чтобы:

- a) используется соответствующий шаблон, доступный на странице конфиденциальности данных во внутренней сети; или
- b) уже заключено внутригрупповое соглашение об обработке данных.

пример

Если Getinge IT оказывает поддержку Getinge HR, которая включает в себя то, что Getinge IT обрабатывает персональные данные от имени Getinge HR, необходимо заключить внутригрупповое соглашение об обработке данных. В данном случае Getinge IT является обработчиком данных, а Getinge HR - контролером данных.

12. Технические и организационные меры безопасности

Все компании Getinge обязаны соблюдать политику и директивы Getinge в отношении информационной безопасности. Компании Getinge также должны принять соответствующие технические и организационные меры для обеспечения уровня безопасности, соответствующего риску. При осуществлении таких мер следует принимать во внимание следующее:

- a) Самый современный;
- b) Стоимость внедрения;
- c) Характер, объем и цели обработки; и
- d) Риск вероятности и серьезности для прав и свобод субъектов данных.

Каждая компания Getinge несет ответственность за обеспечение соответствия обработки персональных данных законам о защите данных, включая принятие соответствующих технических и организационных мер, таких как права доступа, пометка персональных данных для удаления, автоматическое удаление и регистрация данных. Что касается прав доступа, компании Getinge должны обеспечить, чтобы доступ к персональным данным отражал роли сотрудников и консультантов, в том числе в случаях изменения ролей в Getinge.

13. ИТ-решения, обрабатывающие персональные данные

Каждая компания Getinge несет ответственность за обеспечение того, чтобы новые и существующие ИТ-функции, решения и/или сервисы, используемые для обработки персональных данных, соответствовали законам о защите данных, включая, но не ограничиваясь, требованиями, касающимися:

- a) Конфиденциальность по замыслу и по умолчанию;
- b) Хранение данных;
- c) Запросы субъекта данных, включая переносимость данных;
- d) Достаточные технические и организационные меры безопасности; и
- e) Права доступа.

Перед использованием нового ИТ-решения и перед внесением изменений в существующее ИТ-решение компании Getinge должны своевременно информировать Отдел по защите данных о рисках конфиденциальности, целях и обрабатываемых персональных данных. Отделу защиты персональных данных также должна быть предоставлена информация об обработке персональных данных в существующих ИТ-решениях.

Смотрите далее: Директива по информационной безопасности

14. Конфиденциальность по замыслу и по умолчанию

Принципы конфиденциальности по замыслу и по умолчанию должны приниматься во внимание при разработке, проектировании, выборе и использовании приложений, сервисов и продуктов, которые включают обработку персональных данных. Эти принципы должны соблюдаться как во время определения средств обработки, так и во время самой обработки.

Privacy by design - это концепция и подход к проектированию систем, которые учитывают защиту данных на протяжении всего процесса проектирования. Privacy by design фокусируется на обеспечении того, чтобы конфиденциальность с самого начала была встроена в информационные технологии, бизнес-процессы, физические пространства и сетевую инфраструктуру.

Getinge должна обеспечить, чтобы их системы и процессы были специально разработаны с учетом защиты данных. Защита данных не должна быть второстепенной задачей, а должна быть встроена в структуру того, как организация ведет свой бизнес.

Конфиденциальность по умолчанию означает, что Контролер данных должен внедрить механизмы для обеспечения того, чтобы по умолчанию обрабатывались только

необходимые персональные данные для каждой конкретной цели обработки и, в частности, не собирались и не сохранялись сверх того, что необходимо для этих целей, как с точки зрения объема данных, так и времени хранения. В частности, внедренные механизмы должны гарантировать, что персональные данные по умолчанию не будут доступны неопределенному кругу лиц.

пример

В качестве примера, было бы уместно учитывать конфиденциальность по замыслу и по умолчанию, когда Getinge создает новые ИТ-системы для хранения персональных данных или доступа к ним, разрабатывает политику или стратегии, которые влияют на конфиденциальность данных, инициирует обмен персональными данными или их использование в новых целях.

Разработка проектов, процессов, продуктов или систем с учетом конфиденциальности по замыслу и по умолчанию с самого начала имеет ряд преимуществ, в том числе:

- a) Возможность выявлять потенциальные проблемы на ранней стадии, когда их решение часто оказывается более простым и менее затратным;
- b) Повышается осведомленность о конфиденциальности данных во всей организации;
- c) Повышается вероятность выполнения обязательств, предусмотренных законами о защите данных, и в равной степени снижается вероятность нарушений; и
- d) Проекты, процессы, продукты или системы с меньшей вероятностью нарушают неприкосновенность частной жизни и оказывают негативное воздействие на отдельных людей.

Особенно, когда Getinge разрабатывает продукты и услуги, связанные с персональными данными, следует определить соответствующие детали о том, как Getinge должна соблюдать требования конфиденциальности по замыслу и по умолчанию.

15. Утечка персональных данных

Обо всех нарушениях персональных данных должно быть немедленно сообщено в соответствии с процессом, описанным на странице конфиденциальности данных во внутренней сети.

Приобретающие компании должны:

- a) убедитесь, что все решения, используемые для обработки персональных данных, позволяют сообщать о нарушениях персональных данных;
- b) внедрять меры, способствующие выявлению утечек персональных данных;
- c) документируйте обстоятельства нарушения персональных данных, включая последствия, возможные риски и принятые или планируемые средства правовой защиты; и
- d) сотрудничайте с командой по защите персональных данных при расследовании и устранении нарушений персональных данных.

Смотрите далее: Директива о защите персональных данных

16. Надзорные органы

Всеми контактами с надзорными органами должна заниматься группа по защите персональных данных. Компании Getinge должны сотрудничать с надзорными органами по запросу.

17. Отклонения

Отклонения от настоящей Глобальной политики должны утверждаться на том же уровне полномочий, что и при первоначальном утверждении Глобальной политики.

18. Нарушения глобальной политики – Высказывайтесь

Не стесняйтесь высказывать свое беспокойство. Ожидается, что любой сотрудник Getinge, который подозревает нарушения этой глобальной политики, выскажется и поднимет проблему перед своим линейным менеджером, в Отдел этики и соблюдения нормативных требований или воспользуется прямой линией Getinge Speak Up. Линия Getinge Speak Up доступна на внутренних и внешних веб-страницах Getinge. В Getinge мы не принимаем никаких форм возмездия в отношении тех, кто высказывается, выражает озабоченность или мнение.

Смотрите далее: Глобальная директива о гласности и отказе от возмездия

19. Роли и обязанности

Все сотрудники Getinge несут индивидуальную ответственность за чтение, понимание и соблюдение этой Глобальной политики. Каждый сотрудник несет ответственность за действия в соответствии с этой Глобальной политикой.

Каждый линейный менеджер несет ответственность за то, чтобы каждый член команды имел доступ к этой Глобальной политике и связанным с ней директивам, инструкциям и руководящим принципам.

Ежедневное усиление, включая регулярное информирование и обучение в области конфиденциальности данных, а также контроль за соблюдением требований, является частью ответственности каждого менеджера.

Нарушения этой Глобальной политики могут привести к дисциплинарным взысканиям, вплоть до увольнения.

20. Руководство и помощь

Чтобы направлять наше поведение, когда речь заходит о позициях Getinge в области конфиденциальности данных, существует настоящая Глобальная политика и несколько директив и инструкций. Если у вас есть вопросы по этой Глобальной политике или вы не уверены, какие правила применяются, пожалуйста, свяжитесь со службой защиты данных.

21. Полезные ссылки

Заглавие

Директива о нарушении конфиденциальности персональных данных

Директива по управлению конфиденциальностью данных

Директива по информационной безопасности

Глобальная директива о высказывании и отказе от возмездия
