УТВЕРЖДЕНО

Приказом №04-12ОД

от «25» января 2012 года

Политика обработки персональных данных в ООО «Голдман Сакс»

Москва

2012

1 ВВЕДЕНИЕ

Настоящая Политика обработки персональных данных в ООО «Голдман Сакс» (далее Политика) разработана в соответствии с требованиями нормативно-правовых актов Российской Федерации, регулирующих отношения, связанные с обработкой персональных данных (далее ПД). Политика определяет принципы сбора, обработки, хранения, передачи и защиты ПД физических лиц (далее субъекты ПД) реализуемые в ООО «Голдман Сакс» (далее Компания).

Действие настоящей Политики распространяется на все процессы по сбору, записи, систематизации, накоплению, хранению, уточнению, извлечению, использованию, передаче (распространению, предоставлению, доступу), обезличиванию, блокированию, удалению, уничтожению ПД, осуществляемых как с использованием средств автоматизации, так и без использования таких средств.

В дополнение к настоящей Политике разработаны другие внутренние нормативные документы, регламентирующие отдельные процессы управления ПД.

2 НОРМАТИВНАЯ ДОКУМЕНТАЦИЯ

При определении комплексной системы управления ПД использовались положения и требования следующих нормативно-правовых документов:

- Федеральный закон Российской Федерации от 27 июля 2006 г. №152-ФЗ «О персональных данных»;
- Федеральный закон Российской Федерации от 7 августа 2001 г. № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма»;
- Федеральный закон Российской Федерации от 27 июля 2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон Российской Федерации от 22 октября 2004 г. №125-ФЗ «Об архивном деле в Российской Федерации»;
- Трудовой кодекс Российской Федерации;
- Стандарт Банка России СТО БР ИББС-1.0-2008 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения»;
- Рекомендации в области стандартизации Банка России РС БР ИББС-2.4-2010 «Обеспечение информационной безопасности организаций Банковской системы Российской Федерации. Отраслевая частная модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных организаций Банковской системы Российской Федерации».

3 ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1 Принципы обработки ПД

Обработка ПД осуществляется на основе следующих принципов:

1) обработка ПД осуществляется на законной и справедливой основе;
2) обработка ПД ограничивается достижением конкретных, заранее определенных и законных целей. Не допускается обработка ПД, несовместимая с целями сбора ПД;
3) не допускается объединение баз данных, содержащих ПД, обработка которых осуществляется в целях, несовместных между собой;
4) обработке подлежат только те ПД, которые отвечают целям их обработки;
5) содержание и объем обрабатываемых ПД соответствуют заявленным целям обработки. Обрабатываемые ПД не являются избыточными по отношению к заявленным целям обработки;
6) при обработке ПД обеспечивается точность ПД, их достаточность, а в необходимых случаях и актуальность по отношению к заявленным целям их обработки;
7) данные, которые не являются персональными, обрабатываются аналогично остальным данным Компании, подлежащим защите.

3.2 Сбор персональных данных

Сбор, накопление, хранение, изменение, использование и передача ПД осуществляется при условии наличия согласия субъекта ПД. Исключение составляют случаи, когда в соответствии с действующим законодательством допускается обработка ПД без получения согласия субъекта ПД, а именно:

1) обработка ПД необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей;
2) обработка ПД необходима для осуществления правосудия, исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве;
3) обработка ПД необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект ПД, а также для заключения договора по инициативе субъекта ПД или договора, по которому субъект ПД будет являться выгодоприобретателем или поручителем;
4) обработка ПД необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта ПД, если получение согласия субъекта ПД невозможно;

5) обработка ПД необходима для осуществления прав и законных интересов оператора или третьих лиц, либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта ПД;
6) обработка ПД осуществляется в статистических или иных исследовательских целях, при условии обязательного обезличивания ПД. Исключение составляет обработка ПД в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи, а также в целях политической агитации;
7) осуществляется обработка ПД, доступ неограниченного круга лиц к которым предоставлен субъектом ПД, либо по его просьбе;
8) осуществляется обработка ПД, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.

3.3 Хранение персональных данных

Хранение ПД осуществляется в форме, позволяющей определить субъекта ПД не дольше, чем этого требуют соответствующие цели обработки ПД. Обрабатываемые ПД подлежат уничтожению либо обезличиванию по достижении целей обработки, или в случае утраты необходимости в достижении этих целей.

ПД субъектов могут быть получены, проходить дальнейшую обработку и передаваться как на бумажных носителях, так и в электронном виде.

ПД на бумажных носителях, хранятся в запираемых шкафах или сейфах.

ПД субъектов в электронном виде обрабатываются в компьютерных сетях Компании и аффилированной компании Goldman Sachs International (Великобритания).

3.4 Передача персональных данных третьим лицам

Компания вправе поручить обработку ПД другому лицу с согласия субъекта ПД, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора. При этом Компания в договоре обязует лицо, осуществляющее обработку ПД по поручению Компании, соблюдать принципы и правила обработки ПД, предусмотренные федеральным законом №152-ФЗ «О персональных данных».

В случае если Компания поручает обработку ПД другому лицу, ответственность перед субъектом ПД за действия указанного лица несет Компания. Лицо, осуществляющее обработку ПД по поручению Компании, несет ответственность перед Компанией.

Компания обязуется и обязует иные лица, получившие доступ к ПД, не раскрывать третьим лицам и не распространять ПД без согласия субъекта ПД, если иное не предусмотрено законом.

3.5 Трансграничная передача персональных данных

Трансграничная передача ПД может осуществляться в соответствии с требованиями законодательства РФ и только на территорию иностранных государств, обеспечивающих адекватную защиту прав субъектов ПД.

3.6 Уничтожение персональных данных

В случае достижения цели обработки ПД Компания прекращает обработку ПД, если иное не предусмотрено соглашением между Компанией и субъектом персональных данных.

В случае отзыва субъектом ПД согласия на обработку своих ПД Компания прекращает их обработку, если иное не предусмотрено соглашением между Компанией и субъектом ПД, либо если Компания вправе осуществлять обработку ПД без согласия субъекта ПД на основаниях, предусмотренных законом «О персональных данных» или другими федеральными законами.

В случае выявления неправомерной обработки ПД Компания предпринимает меры по уничтожению этих ПД в срок, не превышающий семи рабочих дней со дня выявления неправомерной обработки ПД.

В случае отсутствия возможности уничтожения ПД в течение указанного срока, Компания осуществляет блокирование таких ПД и обеспечивает уничтожение ПД в срок, не превышающий 6 месяцев со дня выявления неправомерной обработки ПД, если иной срок не установлен федеральным законодательством.

В случае если уничтожение ПД было произведено по результатам обработки обращения субъекта ПД и (или) запроса уполномоченного органа по защите прав субъектов ПД, о предпринятых действиях Компания уведомляет субъекта ПД и (или) уполномоченный орган по защите прав субъектов ПД.

ПД на бумажных носителях уничтожаются с помощью средств, гарантирующих невозможность восстановления носителя или посредством вычеркивания (вымарывания и т.п.) ПД.

Уничтожение информации с машиночитаемых носителей ПД, пришедших в негодность или утративших практическую ценность, производится способом, исключающим возможность использования и восстановления информации.

Уничтожение ПД производится в соответствии с актуальными внутренними процессами Компании.

3.7 Защита персональных данных

При обработке ПД Компания принимает необходимые правовые, организационные и технические меры для защиты ПД от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПД, а также от иных неправомерных действий в отношении ПД.

Обеспечение безопасности ПД достигается, в частности:

1) определением угроз безопасности ПД при их обработке в информационных системах персональных данных (далее ИСПДн);
2) применением организационных и технических мер по обеспечению безопасности ПД при их обработке в ИСПДн, необходимых для выполнения требований к защите ПД, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности ПД;
3) оценкой эффективности принимаемых мер по обеспечению безопасности ПД до ввода в эксплуатацию ИСПДн;
4) обнаружением фактов несанкционированного доступа к ПД и принятием необходимых мер;

5) установлением правил доступа к ПД, обрабатываемых в ИСПДн, а также обеспечением регистрации доступа к ПД в ИСПДн;
6) контролем за принимаемыми мерами по обеспечению безопасности ПД и уровня защищенности ИСПДн.

4 ДОСТУП К ПЕРСОНАЛЬНЫМ ДАННЫМ

4.1 Общие положения

Компания обеспечивает конфиденциальность ПД, то есть не допускает их распространения без согласия субъекта ПД или наличия иного законного основания. Обеспечение конфиденциальности обезличенных и общедоступных ПД осуществляется аналогично обеспечению конфиденциальности иных данных, обрабатываемых в Компании.

4.2 Организация внутреннего доступа сотрудников к персональным данным

В рамках данной Политики под внутренним доступом понимается доступ к ПД, предоставляемый сотрудникам Компании.

Доступ к ПД предоставляется только тем сотрудникам Компании, которым ПД необходимы для исполнения их непосредственных должностных обязанностей.

Допуск сотрудников Компании к обработке ПД осуществляется на основании утвержденного Перечня структурных подразделений, сотрудники которых допущены к работе с ПД обрабатываемыми в Компании. Сотрудник Компании допускается к обработке ПД только в том случае, если занимаемая им должность указана в Перечне и только в рамках тех задач, которые он обязан осуществлять для поддержания бизнес-процессов Компании.

Сотрудник Компании допускается к обработке ПД только после ознакомления с внутренними нормативными документами Компании, регламентирующими обработку ПД, и при наличии в его трудовом договоре соответствующего раздела о защите ПД.

4.3 Организация доступа субъектов персональных данных к своим персональным данным

Компания обеспечивает доступ субъектов ПД к принадлежащим им ПД. Для получения такого доступа субъекту ПД необходимо направить в Компанию письменный запрос по форме, приведенной в Приложении А. Компания осуществляет предоставление ПД обратившегося субъекта в доступной для субъекта форме, и с обеспечением отсутствия в них ПД, относящихся к другим субъектам.

В соответствии с законом №152-ФЗ «О персональных данных» субъект ПД имеет право:

1. Получить сведения касающиеся обработки ПД Компанией, а именно:
   - подтверждение факта обработки ПД Компанией;
   - правовые основания и цели обработки ПД;

- цели и применяемые Компанией способы обработки ПД;
- наименование и место нахождения Компании, сведения о лицах (за исключением работников Компании), которые имеют доступ к ПД;
- обрабатываемые ПД, относящиеся к соответствующему субъекту ПД, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
- сроки обработки ПД, в том числе сроки их хранения;
- информацию об осуществленной или предполагаемой трансграничной передаче ПД;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку ПД по поручению оператора, если обработка поручена или будет поручена такому лицу;
- иные сведения, предусмотренные законом «О персональных данных».

2. Потребовать от Компании уточнения его ПД, их блокирования или уничтожения в случае, если ПД являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки;
3. Заявить возражение против принятия в отношении себя решений, порождающих юридические последствия на основе исключительно автоматизированной обработки ПД;
4. Отозвать согласие на обработку ПД в предусмотренных законом случаях.

Право субъекта ПД на доступ к своим данным ограничивается в случае, если:

- обработка ПД осуществляется в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем и финансированию терроризма;
- предоставление ПД нарушает права и законные интересы других лиц.

5 ОТВЕТСТВЕННОСТЬ

Комитет по операционным рискам Компании несет ответственность за организацию защиты прав субъектов ПД в соответствии с требованиями законодательства РФ.

Комитет по операционным рискам делегирует свои полномочия по организации и обеспечению защиты ПД на ежедневной основе следующим образом:

1. Ответственный за организацию обработки ПД осуществляет:
   - надлежащий контроль за соблюдением организацией и ее работниками требований законодательства Российской Федерации о ПД, в том числе требований к защите ПД;
   - организацию работ по подготовке внутренних документов по обработке ПД и вынесение их на согласование и утверждение;

- координацию работ по обеспечению соответствия бизнес-процессов и внутренних нормативных документов Компании требованиям законодательства РФ в области защиты ПД;
- доведение до сведения работников положений законодательства Российской Федерации о ПД, локальных актов по вопросам обработки ПД, требований к защите ПД;
- контроль за приемом и обработкой обращений и запросов субъектов ПД или их представителей, а также уполномоченного органа по защите ПД;
- вынесение на рассмотрение Комитета по операционным рискам вопросов, указанных выше.

2. Отдел информационной безопасности осуществляет:
   - организацию работ Компании по созданию системы защиты ИСПДн соответствующей требованиям законодательства РФ и бизнес-потребностями Компании;
   - поддержание нормативной документации, содержащей описание процедур и технических средств обеспечения информационной безопасности, в актуальном состоянии;
   - контроль предоставления доступа сотрудников к ПД, обрабатывающихся в ИСПДн Компании;
   - приостановление возможности доступа сотрудников Компании к ПД в случае нарушения ими требований внутренних нормативных документов в области защиты ПД.
3. Руководители структурных подразделений, предоставляющих (согласующих) доступ сотрудников к ПД, несут персональную ответственность за обоснованность данного доступа.

К сотрудникам Компании, не исполняющим по своей вине возложенных на них обязанностей по соблюдению порядка работы с ПД, могут применяться дисциплинарные взыскания в соответствии с Трудовым Кодексом.

Сотрудники Компании, виновные в нарушении норм, регулирующих получение, обработку и защиту ПД, несут дисциплинарную, административную, гражданско-правовую, уголовную и иную ответственность в соответствии с законодательством РФ.

ПРИЛОЖЕНИЕ А. ШАБЛОН ЗАПРОСА СУБЪЕКТА ПД

В ООО «Голдман Сакс»
Адрес: Москва, ул.Гашека, 6

Запрос на предоставление информации об обработке персональных данных

От _____
(фамилия, имя, отчество)

паспорт _____ выданный _____
(серия, номер) (дата выдачи)

_____
(место выдачи паспорта)

адрес: _____
(адрес места жительства)

Основания, по которым лицо выступает в качестве законного представителя субъекта персональных данных:

_____

Сведения, подтверждающие факт обработки персональных данных в ООО «Голдман Сакс»:

_____

_____

В соответствии со ст. 14 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных» прошу предоставить следующую информацию*, касающуюся обработки моих персональных данных:

- ☐ подтвердить факт обработки моих персональных данных;
- ☐ правовые основания и цели обработки моих персональных данных;

_____

*отметить нужные пункты

- ☐ наименование и местонахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к моим персональным данным или которым могут быть раскрыты мои персональные данные на основании договора или на основании федерального закона;
- ☐ относящиеся ко мне обрабатываемые персональные данные, источник их получения;
- ☐ сроки обработки моих персональных данных, в том числе сроки их хранения;
- ☐ информацию об осуществленной или предполагаемой трансграничной передаче моих персональных данных;
- ☐ наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку моих персональных данных, если обработка поручена или будет поручена такому лицу
- ☐ _____.

(иные сведения)

Данный запрос является первичным / повторным, на основании того, что:

_____

(ОБЯЗАТЕЛЬНО: указать причину направления повторного запроса)

Указанные сведения прошу предоставить по адресу:

_____

_____

_____

(дата) (подпись)