Консалтинговая компания «Пойнтлэйн»
109012, Москва, ул. Ильинка 4
(495) 233-65-08
contact@pointlane.ru
www.pointlane.ru

Microsoft Office 365

Соответствие требованиям законодательства Российской Федерации

Соответствие обработки персональных данных с использованием Microsoft Office 365 требованиям законодательства Российской Федерации в области персональных данных

Оглавление

О компании Pointlane

Компания «Pointlane» – российская консалтинговая компания, предоставляющая услуги в области информационной безопасности для бизнеса. Компания «Pointlane» была основана в 2008 году командой профессионалов, имеющих обширный опыт в решении комплексных задач по обеспечению информационной безопасности.

Миссия компании «Pointlane» – оказание высококачественных услуг в области информационной безопасности, создающих условия для безопасного ведения бизнеса.

Все сотрудники компании «Pointlane» являются высококвалифицированными специалистами с большим практическим опытом работы по обеспечению информационной безопасности в различных государственных и коммерческих организациях, имеют профильное образование в области защиты информации и информационных технологий, а также обладают рядом сертификатов, таких как CISA, CISSP, MCTS, MCSA:Security, MCSE:Security, PMP. Подготовка сотрудников компании «Pointlane» непрерывно совершенствуется, сотрудники проходят различные тренинги и курсы повышения квалификации.

Проектный опыт компании «Pointlane» включает в себя выполнение работ для различных секторов экономики, от небольших до крупнейших транснациональных компаний по аудиту информационной безопасности, тестированию на проникновение, проектированию и внедрению систем управления информационной безопасности, защиты персональных данных, защиты коммерческой тайны.

Компания «Pointlane» обладает всеми необходимыми лицензиями ФСТЭК и ФСБ для осуществления своей деятельности:

- лицензия ФСТЭК №1427 «На деятельность по технической защите конфиденциальной информации»;
- лицензия ФСБ №10476Р «На осуществление распространения шифровальных (криптографических) средств»;
- лицензия ФСБ №10475Х «На осуществление технического обслуживания шифровальных (криптографических) средств»;
- лицензия ФСБ №10474П «На осуществление разработки, производства шифровальных (криптографических) средств, защищенных с использованием шифровальных (криптографических) средств информационных и телекоммуникационных систем.

ПЕРЕЧЕНЬ ОБОЗНАЧЕНИЙ И СОКРАЩЕНИЙ

AD – Active Directory

ЕС – Европейский союз

Оператор (Клиент) – лицо, осуществляющее обработку персональных данных с использованием Microsoft Office 365

ПДн – персональные данные

Роскомнадзор (Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций) – орган исполнительной власти Российской Федерации, который осуществляет контроль и надзор за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных

РФ – Российская Федерация

ФСБ России (Федеральная служба безопасности) – федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности

ФСТЭК России (Федеральная служба по техническому и экспортному контролю) – федеральный орган исполнительной власти, уполномоченный в области противодействия техническим разведкам и технической защиты информации

ЦОД – центр обработки данных

152-ФЗ – Федеральный закон «О персональных данных» от 27 июля 2006 г. №152-ФЗ

184-ФЗ – Федеральный закон «О техническом регулировании» от 27 декабря 2002 г. №184-ФЗ

294-ФЗ – Федеральный закон «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля» от 26 декабря 2008 г. №294-ФЗ

История документа

Дата	*Версия*	*Статус*	*Комментарий*
Декабрь 2013	0.1	Draft	Создание документа по запросу клиента
Январь 2014	0.2	Draft	Изменения в порядке трансграничной передачи Правки редактора
Март 2014	1	Release	Верстка документа

Авторы документа

Роль	*Имя*	*E-mail*	*Телефон*
Автор	Кайсина Е.	e.kaysina@pointlane.ru	+7(495)233-65-08
Юридическая поддержка	Гаврикова Е.	e.gavrokiva@pointlane.ru	+7(495)233-65-08
Редактор	Лебедев В.	v.lebedev@pointlane.ru	+7(495)233-65-08

Введение

Microsoft Office 365 – это облачное решение Компании Microsoft, позволяющее получить доступ к знакомым средствам Office практически отовсюду благодаря интернет-хранилищу, а также предоставляющее возможность общего доступа и другие возможности для корпоративных клиентов.

Наряду с большим количеством преимуществ облачного решения, перед провайдером такого сервиса стоит сложная задача управления безопасностью. Компания Microsoft использует методики, процессы и технологии, позволяющие обеспечить безопасность Microsoft Office 365.

Microsoft Office 365 может эффективно использоваться организациями, которые являются представителями практически любой отрасли, в том числе со строгим нормативным регулированием. Так как в любой организации, функционирующей на территории РФ, независимо от сферы ее деятельности, обрабатываются персональные данные (далее – ПДн) (к примеру, каждая организация обрабатывает ПДн своих работников), то в первую очередь должна быть рассмотрена проблема соответствия процессов обработки ПДн с использованием Microsoft Office 365 требованиям законодательства РФ в области обработки и защиты ПДн.

В настоящем документе описаны схема и участники взаимодействия, возникающего при использовании Microsoft Office 365, а также требования, предъявляемые к участникам. Затем рассмотрен порядок выполнения обязательных требований в рамках соответствия законодательству в области обработки и защиты ПДн на территории РФ. В результате показано, что использование Microsoft Office 365 не противоречит законодательству РФ в связи с тем, что Компания Microsoft выполняет все возложенные на него обязательства, при этом и Клиенту в свою очередь нетрудно выполнить все необходимые требования, возникающие при использовании Microsoft Office 365.

Многие Операторы (Клиенты) решают использовать для обработки ПДн Microsoft Office 365 вместо использовавшегося до этого локального решения. Российские клиенты, заключая договор с Компанией Microsoft, физически расположенной в Ирландии, беспокоятся о возможных проблемах соответствия требованиям 152-ФЗ при использовании Microsoft Office 365.

Далее описаны возникающие проблемы соответствия требованиям 152-ФЗ и возможности их решения.

СХЕМА И УЧАСТНИКИ ВЗАИМОДЕЙСТВИЯ

Участниками взаимодействия являются:

- **Субъекты ПДн** – физические лица, чьи ПДн обрабатываются в Microsoft Office 365;
- **Клиент** – оператор ПДн субъектов ПДн, использующий Microsoft Office 365;
- **Компания Microsoft** – владелец ЦОД, обрабатываемых в Microsoft Office 365 и провайдер сервиса Microsoft Office 365;
- **Роскомнадзор, ФСТЭК России и ФСБ России** – регуляторы, которые осуществляют контроль и надзор за соответствием обработки ПДн и защиты ПДн требованиям законодательства РФ.

Схема взаимодействия участников при использовании Microsoft Office 365 представлена на Рисунке 1.

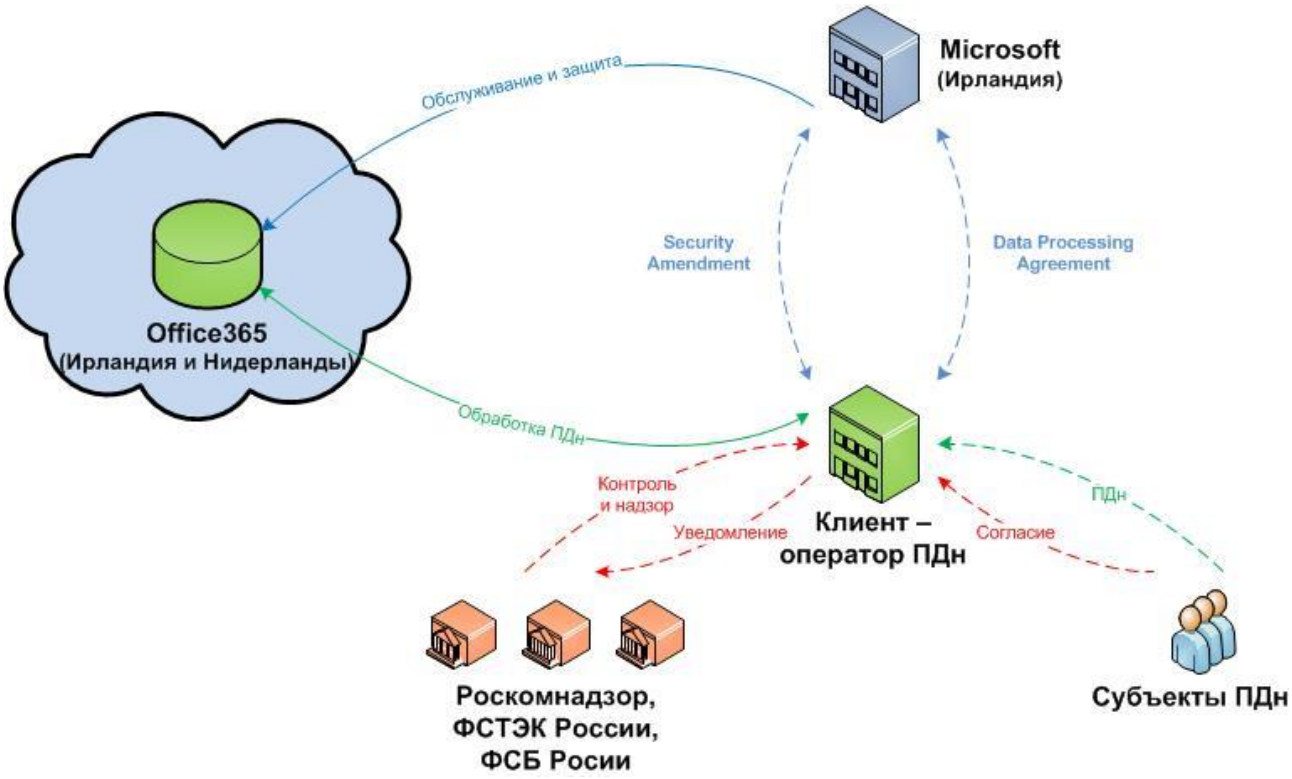

Рисунок 1. Схема взаимодействия участников

ОБЩЕЕ ОПИСАНИЕ ТРЕБОВАНИЙ

Примечание: Данный раздел описывает требования к любому оператору ПДн, безотносительно использования им Microsoft Office 365 для обработки ПДн.

Обработка ПДн влечет за собой возникновение следующих обязанностей для любого оператора ПДн:

1) Соблюдать принципы и условия обработки ПДн [статьи 5 и 6 152-ФЗ]

   Принципы и условия обработки ПДн заключаются в следующем: обработка ПДн должна осуществляться на законной и справедливой основе; обработка ПДн должна осуществляться в строгом соответствии с заявленными целями.

   Включение в процесс обработки Microsoft Office 365 влечет возникновение обязанности по соблюдению провайдером облачного сервиса принципов и условий обработки ПДн, аналогично обязанности оператора ПДн (клиента).

2) Соблюдать конфиденциальность ПДн [статья 7 152-ФЗ]

   Соблюдение конфиденциальности ПДн заключается в не раскрытии ПДн третьим лицам и не распространении их без согласия субъекта ПДн.

   Включение в процесс обработки Microsoft Office 365 влечет возникновение обязанности по соблюдению провайдером облачного сервиса конфиденциальности ПДн, аналогично обязанности оператора ПДн (клиента).

3) Выполнять обязанности к созданию общедоступных источников ПДн [статья 8 152-ФЗ]

   Обязанности к созданию общедоступных источников ПДн (справочников и адресных книг) включают получение согласия субъекта ПДн на включение его ПДн в такие источники и обеспечение возможности исключения ПДн из указанных источников по требованию субъекта ПДн.

4) Выполнять обязанности к обработке специальных категорий ПДн [статья 10 152-ФЗ]

   Обязанности к обработке специальных категорий ПДн (ПДн, касающихся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья и интимной жизни) включают получение согласия субъекта ПДн на обработку таких ПДн или подтверждение законных и необходимых для субъекта ПДн оснований обработки таких ПДн.

5) Выполнять обязанности к обработке биометрических ПДн [статья 11 152-ФЗ]

   Обязанности к обработке биометрических ПДн (ПДн, характеризующих физиологические и биологические особенности человека и использующихся для установления его личности) включают получение согласия субъекта ПДн на обработку таких ПДн или подтверждение законных оснований обработки таких ПДн.

6) Выполнять обязанности к трансграничной передаче ПДн [статья 12 152-ФЗ]

Обязанности к трансграничной передаче ПДн (передаче ПДн на территорию иностранных государств иностранным физическим и юридическим лицам) включают получение согласия субъекта ПДн на осуществление такой передачи ПДн или подтверждение адекватной защиты в иностранном государстве, на территорию которого осуществляется передача, прав субъектов ПДн.

Обязанности к трансграничной передаче ПДн могут меняться при использовании Microsoft Office 365 в связи с тем, что серверы ЦОД Microsoft Office 365 расположены за пределами РФ.

7) Реализовывать права субъекта ПДн:

7.1) На доступ к его ПДн [статья 14 152-ФЗ]

Реализация прав субъекта ПДн на доступ к его ПДн заключается в предоставлении ему доступа к его ПДн по его запросу.

7.2) При обработке его ПДн в целях продвижения товаров, работ, услуг на рынке, а также в целях политической агитации [статья 15 152-ФЗ]

Реализация прав субъекта ПДн при обработке его ПДн в целях продвижения товаров, работ, услуг на рынке, а также в целях политической агитации включает получение предварительного согласия субъекта ПДн на осуществление обработки ПДн в указанных целях, а также обеспечение возможности прекращения такой обработки ПДн по требованию субъекта ПДн.

В связи с использованием Microsoft Office 365 обеспечение возможности прекращения обработки ПДн зависит не только от оператора, но и от возможностей, предоставляемых провайдером облачного сервиса.

7.3) При принятии решений на основании исключительно автоматизированной обработки его ПДн [статья 16 152-ФЗ]

Реализация прав субъекта ПДн при осуществлении исключительно автоматизированной обработки его ПДн, порождающей юридические последствия в его отношении, включает получение согласия субъекта ПДн на осуществление такой обработки ПДн, а также разъяснение ему порядка возникновения указанных последствий и обеспечение возможности рассмотрения возражений субъекта ПДн.

8) Выполнять обязанности при сборе ПДн [статья 18 152-ФЗ]

Обязанности при сборе ПДн заключается в разъяснении субъекту ПДн юридических последствий предоставить его ПДн, в предоставлении субъекту ПДн до начала обработки ПДн информации об условиях обработки его ПДн или подтверждении законных оснований не предоставлять такую информацию.

9) Выполнять обязанности при обращении субъекта ПДн [статья 20 152-ФЗ]

Обязанности при обращении субъекта ПДн к оператору ПДн заключается в предоставлении ему информации об условиях обработки его ПДн по его запросу.

10) Выполнять обязанности по устранению нарушений законодательства в области ПДн [статья 21 152-ФЗ]

Обязанности по устранению нарушений законодательства в области ПДн заключаются в прекращении обработки ПДн до устранения выявленных нарушений, последующем устранении нарушений и извещении субъекта ПДн и Роскомнадзора об устранении нарушений.

11) Уведомить Роскомнадзор об обработке ПДн [статья 22 152-ФЗ]

Уведомление Роскомнадзора об обработке ПДн заключается в сообщении ему в установленном порядке актуальной и достоверной информации об обрабатываемых ПДн, условиях их обработки и защиты.

12) Назначить лицо, ответственное за организацию обработки ПДн [статья 22.1 152-ФЗ]

Назначение лица, ответственного за организацию обработки ПДн, заключается в возложении на ответственное лицо обязанностей по приведению процессов и информационных систем обработки ПДн в соответствие с требованиями 152-ФЗ и контроль выполнения таких требований.

13) Обязанности при осуществлении контроля и надзора в отношении оператора ПДн [статья 23 152-ФЗ, 294-ФЗ]

Обязанности при осуществлении контроля и надзора в отношении оператора ПДн заключаются в предоставлении контрольным и надзорным органам (Роскомнадзор, ФСТЭК России и ФСБ России) необходимой информации для выполнения контрольно-надзорных функций, а также в устранении обнаруженных указанными органами нарушений, допущенных при осуществлении обработки ПДн.

14) Обязанности по обеспечению безопасности ПДн [статья 19 152-ФЗ]

Обязанности по обеспечению безопасности ПДн включают выполнение организационных и технических мер, направленных на обеспечение защиты ПДн от неправомерного или случайного доступа к ним.

Включение в процесс обработки Microsoft Office 365 (провайдера облачного сервиса) влечет возникновение обязанности по обеспечению им безопасности ПДн, аналогично обязанности оператора ПДн.

Требования к участникам взаимодействия

При переходе к использованию Microsoft Office 365 для обеспечения соответствия требованиям 152-ФЗ необходимо:

1) Обеспечить выполнение обязанностей, предусмотренных 152-ФЗ, по обработке ПДн:

1.1) Обязанностей, возникающих при трансграничной передаче – **Клиентом**;
1.2) Возможности прекращения обработки ПДн (уничтожения и блокирования) – **Компанией Microsoft** для Клиента;
1.3) Соблюдения принципов и правил обработки ПДн, установленных 152-ФЗ, – **Компанией Microsoft**;

2) Обеспечить выполнение обязанностей, предусмотренных 152-ФЗ, по защите ПДн:

2.1) Конфиденциальность ПДн – **Компанией Microsoft**;
2.2) Безопасность ПДн – **Компанией Microsoft.**

3) Обеспечить актуальное описание способов обработки ПДн – **Клиентом**.

Клиент может обеспечить выполнение указанных требований, установленных 152-ФЗ, на своей стороне – изданием (изменением) локальных актов в области обработки и защиты ПДн, на стороне Компании Microsoft – поручением ей обработки ПДн.

Обеспечение выполнения Клиентом иных обязанностей, установленных 152-ФЗ:

1) Обязанностей к созданию общедоступных источников ПДн;

2) Обязанностей к обработке специальных категорий ПДн;

3) Обязанностей к обработке биометрических ПДн;

4) Обязанности реализовывать права субъекта ПДн:

4.1) На доступ к его ПДн;
4.2) При принятии решений на основании исключительно автоматизированной обработки его ПДн;

5) Обязанностей при сборе ПДн;

6) Обязанностей при обращении субъекта ПДн;

7) Обязанностей по устранению нарушений законодательства в области ПДн;

8) Обязанности уведомить Роскомнадзор об обработке ПДн;

9) Обязанности назначить лицо, ответственное за организацию обработки ПДн;

10) Обязанностей при осуществлении контроля и надзора в отношении оператора ПДн

не меняется вследствие использования облачных технологий для обработки ПДн.

152-ФЗ действует только на территории РФ и неприменим к Microsoft Ирландия и Microsoft Нидерланды, которые участвуют в процессах обработки ПДн при использовании Microsoft Office 365. Поэтому далее говорится не об организации выполнения Компанией Microsoft требований, установленных 152-ФЗ, а об организации выполнения требований, соответствующих (аналогичных) требованиям, установленным 152-ФЗ, которые установлены:

- Конвенцией Совета Европы о защите физических лиц при автоматизированной обработке персональных данных от 28 января 1981 г.;
- Директивой №95/46/ЕС Европейского парламента и Совета Европейского Союза «О защите физических лиц при обработке персональных данных и о свободном обращении таких данных», принятой в г. Люксембурге 24 октября 1995 г.;
- Стандартами ISO 27001 и ISO 27002 (требования в области информационной безопасности).

Выполнение требований, соответствующих (аналогичных) требованиям законодательства РФ в области ПДн, иностранным физическим лицом является достаточным для использования предоставляемого им сервиса для обработки ПДн на территории РФ, т.е. российским оператором ПДн.

Компания Microsoft принимает меры, направленные на выполнение упоминаемых требований, в целях содействия Клиенту в соблюдении требований 152-ФЗ.

Выполнение требований Компанией Microsoft подтверждается следующими документами:

- Microsoft Online Services Data Processing Agreement (Соглашение об обработке данных при предоставлении Online Services);
- Microsoft Online Services Security Amendment;
- Статья «Средства безопасности Office 365» («Office 365 Security WhitePaper»);
- «Стандартные ответы на запросы информации в Microsoft Online Services. Безопасность и конфиденциальность».

ВОЗМОЖНОСТЬ ПРЕКРАЩЕНИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Возможность Клиенту прекратить обработку ПДн (временно или безвозвратно) – возможность удаления, блокирования, изменения любой информации (в том числе ПДн) – в случаях, установленных 152-ФЗ, с использованием Microsoft Office 365 обеспечена Компанией Microsoft (или осуществляется Компанией Microsoft от имени клиента) в соответствии с п.1.c. Microsoft Online Services Data Processing Agreement.

При прекращении использования Клиентом Microsoft Office 365 Компания Microsoft не продолжает обработку ПДн в соответствии с п.1.c. Microsoft Online Services Security Amendment / Microsoft Online Services Data Processing Agreement.

СОБЛЮДЕНИЕ ПРИНЦИПОВ И ПРАВИЛ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Компания Microsoft обязана соблюдать принципы обработки ПДн:

- обработка ПДн на законной и справедливой основе;
- обработка в ПДн в соответствии с заранее определенными и законными целями

и правила обработки ПДн.

В связи с тем, что:

1) 152-ФЗ устанавливает принципы и правила обработки ПДн в соответствии с ратифицированной РФ Конвенцией Совета Европы о защите физических лиц при автоматизированной обработке персональных данных;

2) В государствах, ратифицировавших Конвенцию Совета Европы о защите физических лиц при автоматизированной обработке персональных данных, обеспечивается адекватная защита прав субъектов ПДн в соответствии с п.1 статьи 12 152-ФЗ

можно сделать вывод о том, что Microsoft Ирландия соблюдает принципы и правила обработки ПДн, соответствующие принципам и правилам, установленным 152-ФЗ, так как Ирландия ратифицировала указанную Конвенцию 01 декабря 1993 г.

КОНФИДЕНЦИАЛЬНОСТЬ ПЕРСОНАЛЬНЫХ ДАННЫХ

Компания Microsoft, получив доступ к ПДн, обязана не раскрывать их третьим лицам и не распространять их без согласия субъекта ПДн, если иное не предусмотрено федеральным законом.

Сотрудники Компании Microsoft обязаны соблюдать конфиденциальность любой информации (в том числе ПДн), полученной от Клиента в связи с использованием Клиентом Microsoft Office 365 в соответствии с:

- п.1.f. Microsoft Online Services Data Processing Agreement;
- п.1.f. Microsoft Online Services Security Amendment / Microsoft Online Services Data Processing Agreement;
- LG-01 «Стандартные ответы на запросы информации в Microsoft Online Services. Безопасность и конфиденциальность».

Компания Microsoft в соответствии с п.1.b.(ii) Microsoft Online Services Data Processing Agreement и п.1.b.(ii) Microsoft Online Services Security Amendment / Microsoft Online Services Data Processing Agreement может раскрывать в том числе ПДн правоприменительным органам в соответствии с законом.

Компания Microsoft может привлекать третьих лиц для предоставления части сервисов Microsoft Office 365 от лица Компании Microsoft в соответствии с:

- п.1.g. Microsoft Online Services Data Processing Agreement
- п.1.g. Microsoft Online Services Security Amendment / Microsoft Online Services Data Processing Agreement

в связи с чем указанные третьи лица могут получить доступ в том числе к ПДн.

При этом Компания Microsoft ответственна перед клиентом за соблюдение указанными третьими лицами конфиденциальности и безопасности ПДн в соответствии с:

- п.1.g. Microsoft Online Services Data Processing Agreement
- п.1.g. Microsoft Online Services Security Amendment / Microsoft Online Services Data Processing Agreement.

БЕЗОПАСНОСТЬ ПЕРСОНАЛЬНЫХ ДАННЫХ

Компания Microsoft обязана поручением обработки ПДн выполнять следующие требования к защите ПДн, обрабатываемых в Microsoft Office 365:

1) Нейтрализация актуальных угроз безопасности ПДн

Определение актуальных угроз безопасности информации, в том числе ПДн, осуществляется Компанией Microsoft в рамках программы управления рисками в соответствии с:

- п.4.a.(i)3) Microsoft Online Services Security Amendment /Microsoft Online Services Data Processing Agreement;
- DG-08 и RI-0x «Стандартные ответы на запросы информации в Microsoft Online Services. Безопасность и конфиденциальность»;
- п.3.a.(i)3) Microsoft Online Services Data Processing Agreement.

Нейтрализация актуальных угроз безопасности информации, в том числе ПДн, обеспечивается Компанией Microsoft путем принятия соответствующих технических и организационных мер, внутренних контролей и процедур информационной безопасности, направленных на защиту информации, в том числе ПДн, от случайных потери, уничтожения и изменения, несанкционированного доступа или раскрытия и незаконного уничтожения в соответствии с:

- п.4.a. Microsoft Online Services Security Amendment / Microsoft Online Services Data Processing Agreement;
- п.3.a. Microsoft Online Services Data Processing Agreement.

2) Организация режима обеспечения безопасности помещений, в которых размещены технические средства облачного сервиса Microsoft Office 365, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения

Организация режима обеспечения безопасности помещений, в которых размещены технические средства облачного сервиса Microsoft Office 365, обеспечивается Компанией Microsoft путем ограничения физического доступа к техническим средствам, на которых расположены информации, в том числе ПДн, в соответствии с:

- п.4.a.(iv)1) Microsoft Online Services Security Amendment / Microsoft Online Services Data Processing Agreement;
- п.3.a.(iv)1) Microsoft Online Services Data Processing Agreement.

ЦОД Microsoft Office 365 гарантируют защиту информации от несанкционированного доступа. Персонал имеет доступ в ЦОД в течение 24 часов только для выполнения рабочих задач. Контроль физического доступа осуществляется посредством многочисленных процедур аутентификации (в том числе двухфакторная аутентификация, биометрическая аутентификация) и обеспечения безопасности (локальная служба безопасности, постоянное видеонаблюдение, датчики движения, системами сигнализации) в соответствии с:

- статьей «Средства безопасности Office 365» («Office 365 Security WhitePaper»);
- FS-01 – FS-05 «Стандартные ответы на запросы информации в Microsoft Online Services. Безопасность и конфиденциальность».

3) Обеспечение сохранности носителей ПДн

Сохранность носителей информации, в том числе ПДн, обеспечивается Компанией Microsoft путем инвентаризации электронных носителей информации, в том числе носителей ПДн, в соответствии с:

- п.4.a.(ii) Microsoft Online Services Security Amendment / Microsoft Online Services Data Processing Agreement;
- п.4.a.(iv)2) Microsoft Online Services Security Amendment / Microsoft Online Services Data Processing Agreement;
- FS-08 «Стандартные ответы на запросы информации в Microsoft Online Services. Безопасность и конфиденциальность»;
- п.3.a.(ii)1) Microsoft Online Services Data Processing Agreement;
- п. 3.a.(iv)2) Microsoft Online Services Data Processing Agreement.

Сохранность носителей информации, в том числе ПДн, при их перемещении, использования за пределами организации обеспечивается в соответствии с FS-06 – FS-08 «Стандартные ответы на запросы информации в Microsoft Online Services. Безопасность и конфиденциальность».

4) Использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства РФ в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз

Даже в тех случаях, когда необходимость применения средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства РФ в области обеспечения безопасности информации, установлена Клиентом, данное требование к защите ПДн неприменимо к Microsoft Ирландия в связи с тем, что 184-ФЗ (федеральный закон, регулирующий отношения, возникающие при оценке соответствия) действует только на территории РФ, и практически не может быть реализовано по отношению к средствам защиты информации, используемым Компанией Microsoft.

5) Назначение должностного лица, ответственного за обеспечение безопасности ПДн в Microsoft Office 365

В связи с тем, что безопасность ПДн при их обработке в Microsoft Office 365 обеспечивает Компания Microsoft, она назначает своего представителя (Privacy Officer) в соответствии с п.1.l. Microsoft Online Services Data Processing Agreement (ответственный за конфиденциальность данных).

6) **Обеспечение возможности доступа к содержанию электронного журнала сообщений исключительно для должностных лиц (работников) уполномоченного лица, которым сведения, содержащиеся в указанном журнале, необходимы для выполнения служебных (трудовых) обязанностей**

В Компании Microsoft ведутся электронные журналы сообщений в соответствии с п.4.a.(v)5). Microsoft Online Services Security Amendment / Microsoft Online Services Data Processing Agreement.

Контроль доступа реализован в Компании Microsoft в соответствии с:

- п.4.a.(vi) Microsoft Online Services Security Amendment / Microsoft Online Services Data Processing Agreement;
- IS-08 – IS-10 «Стандартные ответы на запросы информации в Microsoft Online Services. Безопасность и конфиденциальность»;
- п.3.a.(vi) Microsoft Online Services Data Processing Agreement.

7) **Создание структурного подразделения, ответственного за обеспечение безопасности ПДн в Microsoft Office 365, либо возложение на одно из структурных подразделений функций по обеспечению такой безопасности**

В связи с тем, что безопасность ПДн при их обработке в Microsoft Office 365 обеспечивается Компанией Microsoft, Компания Microsoft выделяет несколько сотрудников (security officers), ответственных за координацию и мониторинг процедур информационной безопасности в соответствии с:

- п. 4.a.(i)1) Microsoft Online Services Security Amendment / Microsoft Online Services Data Processing Agreement;
- п.3.a.(i)1) Microsoft Online Services Data Processing Agreement.

8) **Контроль за выполнением требований к защите ПДн при их обработке в Компании Microsoft Office 365 (не реже 1 раза в 3 года)**

Компания Microsoft по письменному запросу Клиента предоставляет ему выдержки из отчета аудита безопасности, чтобы клиент мог убедиться в том, что Компания Microsoft выполняет возложенные на нее обязательства по выполнению требований к защите информации, в том числе ПДн, в соответствии с:

- п.4.b.(iii) Microsoft Online Services Security Amendment / Microsoft Online Services Data Processing Agreement;
- п.3.b.(iii) Microsoft Online Services Data Processing Agreement.

Ответственность перед Клиентом

При поручении обработки ПДн возникает следующая схема ответственности: **ответственность перед субъектом ПДн несет Клиент, а перед Клиентом – Компанией Microsoft.**

Компания Microsoft осуществляет обработку информации, в том числе ПДн, в строгом соответствии с поручением Клиента в соответствии с п.3. Microsoft Online Services Security Amendment / Microsoft Online Services Data Processing Agreement.

ВЫПОЛНЕНИЯ ОБЯЗАННОСТЕЙ, ВОЗНИКАЮЩИХ ПРИ ТРАНСГРАНИЧНОЙ ПЕРЕДАЧЕ

Основные центры обработки данных Microsoft Office 365, которые используются для предоставления сервисов Microsoft Office 365 в том числе российским клиентам, расположены в Ирландии и Нидерландах. Там же расположены центры обработки данных, которые используются для резервного копирования.

При обработке ПДн с использованием Microsoft Office 365, поручая обработку ПДн Компании Microsoft, Клиент осуществляет первоначальную трансграничную передачу ПДн в Компанию Microsoft на территории следующих иностранных государств:

- Ирландия;
- Нидерланды.

Ирландией и Нидерландами обеспечивается адекватная защита прав субъектов ПДн в связи с тем, что указанные государства являются сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке ПДн, что не приводит к возникновению для Клиента дополнительных обязанностей при использовании им Microsoft Office 365 для обработки ПДн.

Данные AD и Global Address Book (данные учетных записей пользователей Microsoft Office 365) при определенных обстоятельствах и условиях могут передаваться с территории Ирландии или Нидерландов и обрабатываться на территории США, при этом следует иметь в виду следующее:

США не входят в перечень стран, которые Роскомнадзор определил как обеспечивающие адекватную защиту прав субъектов ПДн. Однако следует учитывать, что Европейская комиссия заключила соглашение с Министерством торговли США, согласно которому организации США могут выполнять самостоятельную сертификацию на соответствие требованиям программы «Безопасная гавань» (Safe Harbor) в целях обеспечения бесперебойности передачи данных между странами в рамках международной деловой деятельности, включая передачу ПДн. Сертификация подтверждает выполнение требований к защите ПДн, установленных Директивой №95/46/ЕС Европейского парламента и Совета Европейского Союза «О защите физических лиц при обработке персональных данных и о свободном обращении таких данных», которые, как отмечалось выше, аналогичны требованиям, установленным российским законодательством. Компания Microsoft имеет такие сертификаты, выданные Министерством торговли США. Сертификация по программе «Безопасная гавань» позволяет осуществлять законную передачу ПДн из ЕС в Компанию Microsoft в целях ее обработки, т.к. на передачу ПДн из страны – участницы ЕС будет распространяться право ЕС. При этих условиях на передачу данных с территории стран – участниц ЕС в рамках AD и Global Address Book (данные учетных записей пользователей Microsoft Office 365) дополнительных ограничений в соответствии с европейским законодательством не налагается.

Обеспечение безопасности персональных данных

В связи с тем, что безопасность ПДн при их обработке в Microsoft Office 365 обеспечивает Компания Microsoft в соответствии с поручением обработки ПДн, от Клиента не требуется дополнительных мероприятий по защите ПДн, за исключением мероприятий в отношении конфиденциальности средств связи, связанных с использованием Microsoft Office 365 в соответствии с:

- п.2. Microsoft Online Services Security Amendment / Microsoft Online Services Data Processing Agreement;
- п.2.a. Microsoft Online Services Data Processing Agreement.

Стоит отметить что:

1) Компания Microsoft, предоставляя сервис Microsoft Office 365, обеспечивает высокую доступность обрабатываемых в нем информации, в том числе ПДн;

2) Компания Microsoft применяет систему безопасности на основе серии стандартов ISO/IEC 2700x и имеет соответствующие сертификаты, что означает, что Компания Microsoft реализует меры по обеспечению безопасности информации (в том числе ПДн) при их обработке в Microsoft Office 365 – в соответствии с лучшими мировыми практиками в области информационной безопасности;

3) Компания Microsoft использует методы защищенного программирования при разработке программного обеспечения Microsoft Office 365 (что подтверждается Qualification Guideline for Microsoft Office 365), в связи с чем можно считать неактуальными угрозы, связанные с наличием недокументированных (недекларированных) возможностей в программном обеспечении Microsoft Office 365.

Актуальное описание способов обработки персональных данных

При переходе от необлачного решения к Microsoft Office 365 Клиенту нужно отразить такое изменение способа обработки ПДн в своих локальных нормативных актах. Такую информацию запрашивают регуляторы при осуществлении контроля и надзора за соответствием обработки ПДн требованиям 152-ФЗ.

Выполнение обязанностей, возникающих при поручении обработки персональных данных

Клиент может поручить обработку ПДн Компании Microsoft только с согласия субъекта ПДн и на основании заключаемого с Компанией Microsoft договора.

Клиент должен получить согласия субъектов ПДн на обработку их ПДн в Microsoft Office 365 прежде, чем осуществлять обработку их ПДн с использованием Microsoft Office 365.

В п.2.b. Microsoft Online Services Data Processing Agreement установлена обязанность Клиента получать необходимые согласия.

Выводы

Компания Microsoft осознает необходимость соответствия требованиям законодательства и в соответствии с требованиями лучших практик в области информационной безопасности считает и ПДн, обрабатываемые в Microsoft Office 365, и сам сервис объектом регулирования законодательства.

Компания Microsoft выполняет обязанности, предусмотренные 152-ФЗ для лица, осуществляющего обработку ПДн по поручению оператора (Клиента).

Для обеспечения выполнения всех обязанностей, предусмотренных 152-ФЗ для оператора, использующего для обработки ПДн Microsoft Office 365, Клиенту необходимо:

- собрать согласия с субъектов ПДн, обработка чьих ПДн предполагается в Microsoft Office 365, на поручение обработки их ПДн Компании Microsoft.

В остальном обязанности Клиента, возложенные на него в связи с обработкой ПДн, не изменятся в связи с использованием Microsoft Office 365.