

УТВЕРЖДАЮ
Генеральный директор
ООО «БЛС ИНТЕРНЭШНЛ РУ» Р. Кумар
« 08 » 10 2026 г.



**ПОЛИТИКА
ООО «БЛС ИНТЕРНЭШНЛ РУ»
В ОТНОШЕНИИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ**

г. Москва, 2026 г.

1. Общие положения

Обеспечение конфиденциальности и безопасности обработки персональных данных в обществе с ограниченной ответственностью «БЛС ИНТЕРНЭШНЛ РУ» (далее — Оператор) является одной из приоритетных задач организации.

У Оператора для этих целей введён в действие комплект организационно-распорядительной документации, обязательный к исполнению всеми сотрудниками организации, допущенными к обработке персональных данных.

Обработка, хранение и обеспечение конфиденциальности и безопасности персональных данных осуществляются в соответствии с Конституцией Российской Федерации, Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» (далее — Федеральный закон № 152-ФЗ), Трудовым кодексом Российской Федерации, иными нормативными правовыми актами Российской Федерации в сфере персональных данных и локальными актами Оператора.

Настоящая Политика определяет принципы, порядок и условия обработки персональных данных работников, соискателей, граждан, подающих документы для получения визы и (или) для легализации (апостиля, заверения) документов, контрагентов Оператора и иных лиц, чьи персональные данные обрабатываются Оператором, с целью обеспечения защиты прав и свобод гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну, а также устанавливает ответственность должностных лиц Оператора, имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных.

Поскольку к настоящей Политике в соответствии с частью 2 статьи 18.1 Федерального закона № 152-ФЗ необходимо обеспечить неограниченный доступ, в ней не публикуется детальная информация о принятых мерах по защите персональных данных Оператором, а также иная информация, использование которой неограниченным кругом лиц может нанести ущерб Оператору или субъектам персональных данных.

Настоящая Политика размещается на официальном сайте Оператора, на информационном стенде Оператора, что обеспечивает неограниченный доступ к ней.

Контактные данные ответственного за организацию обработки персональных данных

Для обеспечения соблюдения требований законодательства о персональных данных Оператор назначил ответственного за организацию обработки персональных данных. Сведения для связи с ответственным лицом:

— Должность: ответственный за организацию обработки персональных данных ООО «БЛС ИНТЕРНЭШНЛ РУ»;

— Почтовый адрес: 115054, город Москва, Космодамианская набережная, дом 52 строение 7;

— Адрес электронной почты: info.dme@blshelpline.com;

— +7 902 355 9781

Все запросы, касающиеся обработки персональных данных, включая запросы на доступ, уточнение, блокирование, уничтожение и отзыв согласия, направляются по указанным контактным данным.

Основные понятия, используемые в Политике

персональные данные — любая информация, относящаяся к прямо или косвенно определённому или определяемому физическому лицу (субъекту персональных данных);

оператор персональных данных (оператор) — государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие

цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

обработка персональных данных — любое действие (операция) или совокупность действий (операций) с персональными данными, совершаемых с использованием средств автоматизации или без использования таких средств. Обработка персональных данных включает в себя, в том числе: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение;

автоматизированная обработка персональных данных — обработка персональных данных с помощью средств вычислительной техники;

распространение персональных данных — действия, направленные на раскрытие персональных данных неопределённому кругу лиц;

предоставление персональных данных — действия, направленные на раскрытие персональных данных определённому лицу или определённому кругу лиц;

блокирование персональных данных — временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

уничтожение персональных данных — действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных;

обезличивание персональных данных — действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

информационная система персональных данных — совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

трансграничная передача персональных данных — передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу;

биометрические персональные данные — сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность;

специальные категории персональных данных — персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни гражданина.

2. Состав персональных данных

Сведениями, составляющими персональные данные, является любая информация, относящаяся к прямо или косвенно определённому или определяемому физическому лицу (субъекту персональных данных).

Перечень персональных данных, подлежащих защите, определяется целями их обработки, Федеральным законом № 152-ФЗ, Трудовым кодексом РФ и другими нормативными правовыми актами. У Оператора утверждён перечень персональных данных, подлежащих защите.

Оператор обрабатывает следующие категории персональных данных в зависимости от субъекта и цели обработки:

2.1. Персональные данные работников

Оператор обрабатывает следующие персональные данные работников в целях кадрового учёта, исполнения трудового законодательства и налоговых обязательств:

1. фамилия, имя, отчество;
2. год, месяц, день рождения;
3. место рождения;
4. семейное положение;
5. сведения о доходах;
6. пол;
7. адрес электронной почты;
8. адрес места жительства;
9. адрес регистрации;
10. номер телефона;
11. СНИЛС;
12. ИНН;
13. гражданство;
14. данные документа, удостоверяющего личность;
15. реквизиты банковской карты;
16. номер расчётного счёта;
17. номер лицевого счёта;
18. профессия;
19. должность;
20. сведения о трудовой деятельности (в том числе стаж работы, данные о трудовой занятости на текущее время с указанием наименования и расчётного счёта организации);
21. данные трудового договора;
22. приказы по личному составу;
23. отношение к воинской обязанности, сведения о воинском учёте;
24. сведения об образовании;
25. сведения о состоянии здоровья (в случаях, предусмотренных трудовым законодательством);
26. сведения о судимости (в случаях, предусмотренных законодательством);
27. данные изображения лица, полученные с помощью фото- и видеоустройств, позволяющие установить личность субъекта персональных данных (биометрические персональные данные — обрабатываются при наличии отдельного согласия в соответствии со статьёй 11 Федерального закона № 152-ФЗ);
28. сведения о повышении квалификации и о переподготовке работников;
29. сведения о социальных льготах и гарантиях;
30. сведения об отпусках;
31. код, номер, уровень доступа, время действия, дата выдачи, тип карты доступа в помещения.

2.2. Персональные данные соискателей на вакантные должности

Оператор обрабатывает следующие персональные данные соискателей на вакантные должности:

1. фамилия, имя, отчество;
2. год, месяц, день рождения;
3. семейное положение;

4. пол;
5. адрес электронной почты;
6. адрес места жительства;
7. адрес регистрации;
8. номер телефона;
9. СНИЛС;
10. ИНН;
11. гражданство;
12. данные документа, удостоверяющего личность;
13. профессия;
14. должность;
15. сведения о трудовой деятельности (в том числе стаж работы, данные о трудовой занятости на текущее время с указанием наименования и расчётного счёта организации);
16. отношение к воинской обязанности, сведения о воинском учёте;
17. сведения об образовании;
18. сведения из резюме, не вошедшие в список.

2.3. Персональные данные граждан, подающих документы для получения визы

Оператор обрабатывает следующие персональные данные граждан, подающих документы для получения визы:

1. фамилия, имя, отчество;
2. год, месяц, день рождения;
3. место рождения;
4. семейное положение;
5. социальное положение;
6. имущественное положение;
7. доходы;
8. пол;
9. адрес электронной почты;
10. адрес места жительства;
11. адрес регистрации;
12. номер телефона;
13. СНИЛС;
14. ИНН;
15. гражданство;
16. данные документа, удостоверяющего личность;
 - серия;
 - номер;
 - когда и каким органом выдан;
 - код подразделения.
17. данные документа, удостоверяющего личность за пределами Российской Федерации;
 - номер;
 - дата выдачи;
 - срок действия;
 - кем выдан.
18. данные документа, содержащиеся в свидетельстве о рождении;
19. реквизиты банковской карты;

- 20. номер расчётного счёта;
- 21. номер лицевого счёта;
- 22. сведения о трудовой деятельности или с места учёбы (из подтверждающих документов);

Для работников:

- справка с места работы;
- наименование компании;
- телефон;
- адрес компании;
- дата приёма на работу;
- фактическое место работы;
- должность;
- профессия.

Для фрилансеров:

- копии контрактов на обслуживание;
- оригиналы выписки из банковского счёта.

Для пенсионеров:

- данные пенсионного свидетельства;
- справка из Пенсионного фонда.

Для студентов:

- письмо из университета;
- данные студенческого билета;
- название учебного заведения;
- адрес учебного заведения;
- телефон учебного заведения.

Для школьников:

- письмо из школы;
- название учебного заведения;
- адрес учебного заведения;
- телефон учебного заведения.

Данные об обучении в образовательных учреждениях (из подтверждающих документов):

- свидетельство/приказ/выписка о зачислении;
- документы об оплате учебного курса;
- продолжительность курса;
- описание курса;
- стоимость стипендии;
- диплом;
- диплом о предыдущем образовании;
- портфолио;
- свидетельство об окончании курсов;
- данные о знании иностранного языка;
- рисунки, эскизы (для творческих специальностей);
- мотивационное или рекомендательное письмо.

23. Данные транспортных средств и страховых документов:

- 23.1. данные водительского удостоверения;
- 23.2. свидетельство о регистрации транспортного средства;
- 23.3. данные об арендованном транспортном средстве;

- 23.4. данные договора на аренду транспортного средства;
- 23.5. данные доверенности;
- 23.6. данные паспорта собственника;
- 23.7. данные транспортного средства;
- 23.8. данные паспорта водителя (если применимо);
- 23.9. данные международного страхового полиса;
- 23.10. данные международной медицинской страховки:
 - имя и фамилия застрахованного лица,
 - страховой период путешествия,
 - количество дней,
 - застрахованная территория,
 - страховая сумма.
- 24. Данные приглашающей (принимающей) стороны:
 - 24.1. наименование компании или принимающей организации;
 - 24.2. телефон компании или принимающей организации;
 - 24.3. адрес компании или принимающей организации;
 - 24.4. данные паспорта контактного лица в принимающей компании или организации;
 - 24.5. адрес туристического агентства;
 - 24.6. данные приглашения от физического лица, компании, образовательного учреждения, медицинского учреждения и т. д.
- 25. Данные по коммерческим и трудовым документам:
 - данные договора купли-продажи;
 - данные документов, подтверждающих наличие договорных отношений с приглашающей организацией;
 - данные документов, подтверждающих наличие договорных отношений с отправляющей организацией;
 - личный трудовой договор;
 - контракт;
 - счёт-фактура;
 - накладная;
 - сопроводительное письмо;
 - справка;
 - данные квитанции об оплате консульского сбора;
 - иные документы, необходимые для подтверждения сведений в соответствии с требованиями консульских учреждений.
- 26. Данные для отдельных категорий заявителей:
 - Спортсмены (при наличии разрешения, выданного компетентным органом):
 - анкетные данные атлета;
 - выбранная спортивная дисциплина;
 - данные принимающей стороны.
 - Моряки:
 - удостоверение моряка;
 - мореходная книжка;
 - судовая роль.
 - Религиозные деятели:
 - данные документов, подтверждающих религиозный статус.
 - Лица, запрашивающие постоянное проживание:

— данные мотивационного письма с разъяснением причины для постоянного проживания.

27. Специальные категории персональных данных:

В отдельных случаях для оформления визовых документов (например, медицинская виза) Оператор обрабатывает следующие специальные категории персональных данных, относящиеся к состоянию здоровья заявителя:

- данные медицинской карты;
- эпикриз (выписка из истории болезни);
- тип лечения;
- указание сроков лечения;
- стоимость лечения.

28. сведения о судимости в случаях, предусмотренных законодательством;

29. данные изображения лица, полученные с помощью фото- и видеоустройств, позволяющие установить личность субъекта персональных данных (биометрические персональные данные);

30. изображение папиллярных узоров пальцев рук (биометрические персональные данные);

31. иные биометрические персональные данные, которые могут быть необходимы для оформления визовых документов.

2.4. Персональные данные граждан при регистрации личного кабинета на сайте Оператора

Оператор обрабатывает следующие персональные данные граждан при регистрации личного кабинета на сайте Оператора:

1. фамилия, имя, отчество;
2. год, месяц, день рождения;
3. тип паспорта;
4. страна выдачи паспорта;
5. номер паспорта;
6. дата выдачи паспорта в формате день/месяц/год;
7. дата окончания действия паспорта;
8. номер телефона;
9. город выдачи паспорта;
10. адрес электронной почты.

2.5. Персональные данные граждан, оформивших запись в визовый центр через сайт

Оператор обрабатывает следующие персональные данные граждан, оформивших запись в визовый центр через сайт:

1. фамилия, имя, отчество;
2. фамилия при рождении;
3. дата рождения;
4. город рождения;
5. страна рождения;
6. гражданство;
7. гражданство при рождении;
8. пол;
9. семейное положение;
10. номер национального паспорта;
11. тип заграничного паспорта;

12. номер заграничного паспорта;
13. страна выдачи заграничного паспорта;
14. дата выдачи заграничного паспорта;
15. дата окончания действия заграничного паспорта;
16. адрес места регистрации;
17. номер телефона;
18. наименование организации работодателя;
19. телефон организации работодателя;
20. адрес организации работодателя;
21. должность работодателя;
22. сведения о ранее выданных шенгенских визах (номер визы, срок действия, страна выдачи);
23. сведения о приглашающей стороне (если имеется):
 - наименование организации или фамилия, имя, отчество принимающей стороны;
 - страна, город, полный адрес, контактный телефон принимающей стороны.

В случае если оформляется запись для несовершеннолетнего, дополнительно обрабатываются:

1. фамилия законного представителя;
2. имя законного представителя;
3. отчество законного представителя;
4. гражданство законного представителя;
5. адрес регистрации законного представителя.

Персональные данные членов семьи заявителя, являющихся гражданами Европейского союза, Европейской экономической зоны или Швейцарии:

1. фамилия, имя, отчество (если имеется);
2. дата рождения;
3. гражданство;
4. номер документа, удостоверяющего личность.

В случае если постоянное место жительства отличается от страны гражданства:

1. номер документа, удостоверяющего право пребывания в стране местожительства;
2. срок действия документа, удостоверяющего право пребывания в стране местожительства.

2.6. Персональные данные контрагентов

Оператор обрабатывает следующие персональные данные контрагентов:

1. фамилия, имя, отчество;
2. паспортные данные;
3. адрес электронной почты;
4. номер телефона.

2.7. Персональные данные лиц, подавших документы для легализации (апостиля, заверения)

Оператор обрабатывает следующие персональные данные заявителей, подавших документы для легализации (апостиля, заверения), в зависимости от цели обращения и типа запрашиваемой услуги:

2.7.1. Общие персональные данные:

1. фамилия при рождении;
2. имя при рождении;
3. фамилия;
4. имя;

5. отчество (если имеется);
6. дата рождения (день, месяц, год);
7. место рождения;
8. страна рождения;
9. гражданство;
10. гражданство при рождении;
11. сведения о проживании в стране, отличной от страны текущего гражданства;
12. пол;
13. семейное положение;
14. данные документов, подтверждающих родство;
15. домашний адрес;
16. сведения о регистрации;
17. номер телефона;
18. адрес электронной почты;

Данные несовершеннолетних (при подаче документов на несовершеннолетнего):

1. фамилия;
2. имя;
3. отчество (если имеется);
4. адрес;
5. гражданство;
6. телефон;
7. адрес электронной почты опекуна/законного представителя.

2.7.2. Данные документов, удостоверяющих личность:

Данные паспорта гражданина Российской Федерации:

- серия;
- номер;
- когда и каким органом выдан;
- код подразделения.

Данные заграничного паспорта:

- номер;
- дата выдачи;
- срок действия;
- кем выдан.

2.7.3. Сведения о трудовой деятельности и статусе занятости:

Для работников:

- справка с места работы;
- наименование компании;
- телефон;
- адрес компании;
- дата приёма на работу;
- фактическое место работы;
- должность;
- профессия.

Для фрилансеров:

- копии контрактов на обслуживание;

— оригиналы выписки из банковского счёта.

Для пенсионеров:

- данные пенсионного свидетельства;
- справка из Пенсионного фонда.

Для студентов:

- письмо из университета;
- данные студенческого билета;
- название учебного заведения;
- адрес учебного заведения;
- телефон учебного заведения.

Для школьников:

- письмо из школы;
- название учебного заведения;
- адрес учебного заведения;
- телефон учебного заведения.

2.7.4. Данные транспортных средств и страховых документов:

1. данные водительского удостоверения;
2. свидетельство о регистрации транспортного средства;
3. данные об арендованном транспортном средстве;
4. данные договора на аренду транспортного средства;
5. данные доверенности;
6. данные паспорта собственника;
7. данные транспортного средства;
8. данные паспорта водителя (если применимо);
9. данные международного страхового полиса;
10. данные международной медицинской страховки:
 - имя и фамилия застрахованного лица,
 - страховой период путешествия,
 - количество дней,
 - застрахованная территория,
 - страховая сумма.

2.7.5. Данные об обучении в образовательных учреждениях:

1. свидетельство/приказ/выписка о зачислении;
2. документы об оплате учебного курса;
3. продолжительность курса;
4. описание курса;
5. стоимость стипендии;
6. диплом;
7. диплом о предыдущем образовании;
8. портфолио;
9. свидетельство об окончании курсов;
10. данные о знании иностранного языка;
11. рисунки, эскизы (для творческих специальностей);
12. мотивационное или рекомендательное письмо.

2.7.6. Данные по коммерческим и трудовым документам:

1. данные договора купли-продажи;
2. данные документов, подтверждающих наличие договорных отношений с приглашающей организацией;
3. данные документов, подтверждающих наличие договорных отношений с отправляющей организацией;
4. личный трудовой договор;
5. контракт;
6. счёт-фактура;
7. накладная;
8. сопроводительное письмо;
9. справка;

2.8. Обработка специальных категорий персональных данных

Обработка специальных категорий персональных данных осуществляется Оператором исключительно при наличии отдельного письменного согласия субъекта персональных данных в соответствии со статьёй 10 Федерального закона № 152-ФЗ. Без такого согласия обработка специальных категорий персональных данных не производится.

3. Цели обработки персональных данных

Оператор осуществляет обработку персональных данных в следующих целях:

1. организация кадрового учёта компании, ведение кадрового делопроизводства, исполнение требований налогового законодательства (исчисление и уплата налога на доходы физических лиц, страховых взносов во внебюджетные фонды), пенсионного законодательства при формировании и представлении персонифицированных данных, заполнение первичной статистической документации — в соответствии с Трудовым кодексом РФ, Налоговым кодексом РФ, Федеральным законом «Об индивидуальном (персонифицированном) учёте в системе обязательного пенсионного страхования», Федеральным законом № 152-ФЗ и иными нормативными правовыми актами;
2. подбор кандидатов на вакантные должности;
3. приём, обработка и передача визовых документов в дипломатические/консульские учреждения иностранных государств для оформления виз;
4. приём, обработка и передача документов для легализации (апостиля, заверения) в компетентные органы иностранных государств;
5. обеспечение записи граждан на приём в визовый центр через сайт и личный кабинет;
6. предоставление гражданам информационных сервисов, связанных с статусом их визовых заявлений;
7. исполнение договоров по предоставлению услуг и выполнению работ, заключённых между Оператором и субъектом персональных данных или заказчиком услуг.

4. Правовые основания обработки персональных данных

Оператор обрабатывает персональные данные на основании следующих правовых оснований, предусмотренных частью 1 статьи 6 Федерального закона № 152-ФЗ:

1. пункт 1 части 1 статьи 6 — согласие субъекта персональных данных на обработку его персональных данных (для обработки персональных данных граждан, подающих документы для получения визы или для их легализации, соискателей, контрагентов, а также при обработке биометрических и специальных категорий персональных данных);

2. пункт 2 части 1 статьи 6 — обработка персональных данных 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 (для обработки персональных данных работников в рамках трудового законодательства, налогового учёта, пенсионного страхования);

3. пункт 3 части 1 статьи 6 — обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или в случаях, предусмотренных федеральным законом, при предоставлении субъектом персональных данных согласия на обработку (для исполнения договоров по предоставлению визовых и сопутствующих услуг);

4. пункт 5 части 1 статьи 6 — обработка персональных данных 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 персональных данных.

Обработка биометрических персональных данных осуществляется на основании статьи 11 Федерального закона № 152-ФЗ при наличии отдельного письменного согласия субъекта персональных данных.

Обработка специальных категорий персональных данных (данные о состоянии здоровья) осуществляется на основании статьи 10 Федерального закона № 152-ФЗ при наличии отдельного письменного согласия субъекта персональных данных.

Трансграничная передача персональных данных осуществляется при наличии согласия субъекта персональных данных на трансграничную передачу в соответствии со статьёй 12 Федерального закона № 152-ФЗ.

5. Сроки обработки персональных данных

Сроки обработки персональных данных определяются в соответствии со сроком действия договора (соглашения) с субъектом персональных данных, Приказом Росархива от 20 декабря 2019 года № 236 «Об утверждении Перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков их хранения», сроком исковой давности, а также иными требованиями законодательства Российской Федерации.

У Оператора создаются и хранятся документы, содержащие сведения о субъектах персональных данных. Требования к использованию у Оператора данных типовых форм документов установлены Постановлением Правительства РФ от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» в действующей редакции.

5.1. Уничтожение персональных данных

Уничтожение персональных данных производится:

1. по достижении целей обработки персональных данных;
2. в случае утраты необходимости в достижении целей обработки;
3. при отзыве субъектом персональных данных согласия на обработку;
4. по истечении сроков хранения, установленных законодательством Российской Федерации.

Уничтожение персональных данных осуществляется комиссией, назначаемой приказом Оператора, с составлением акта об уничтожении персональных данных в соответствии с локальным актом Оператора, регулирующим порядок уничтожения персональных данных.

5.2. Локализация персональных данных

В соответствии со статьей 18.5 Федерального закона № 152-ФЗ, введенной Федеральным законом от 21 июля 2022 года № 266-ФЗ «О внесении изменений в Федеральный закон «О персональных данных», отдельные законодательные акты Российской Федерации и признании утратившей силу части четырнадцатой статьи 30 Федерального закона «О банках и банковской деятельности» запись, систематизация, накопление, хранение, уточнение и извлечение персональных данных граждан Российской Федерации, предоставляемых Оператору, осуществляются с использованием баз данных, находящихся на территории Российской Федерации (требование действует с 1 июля 2025 года).

6. Права и обязанности

6.1. ООО «БЛС ИНТЕРНЭШНЛ РУ» как оператор персональных данных вправе:

1. отстаивать свои интересы в суде;
2. предоставлять персональные данные субъектов третьим лицам, если это предусмотрено действующим законодательством (налоговые, правоохранительные органы и др.);
3. отказывать в предоставлении персональных данных в случаях, предусмотренных законодательством Российской Федерации;
4. использовать персональные данные субъекта без его согласия в случаях, предусмотренных законодательством Российской Федерации;
5. требовать подтверждения личности в любой не противоречащей закону форме.

6.2. ООО «БЛС ИНТЕРНЭШНЛ РУ» как оператор персональных данных обязан:

1. обеспечить каждому субъекту персональных данных возможность ознакомления с документами и материалами, содержащими его персональные данные, если иное не предусмотрено законом;
2. внести необходимые изменения, уничтожить или заблокировать персональные данные в случае предоставления субъектом неполных, устаревших, недостоверных или незаконно полученных персональных данных, а также уведомить о своих действиях субъекта персональных данных;
3. выполнять требования законодательства Российской Федерации;
4. опубликовать настоящую Политику и сведения о реализуемых требованиях к защите персональных данных, а также контактные данные ответственного за организацию обработки персональных данных;
5. принимать необходимые правовые, организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа, уничтожения, изменения, блокирования, копирования, предоставления, распространения и иных неправомерных действий.

6.3. Субъект персональных данных имеет право:

1. получать информацию, касающуюся обработки его персональных данных, в соответствии со статьей 14 Федерального закона № 152-ФЗ; в том числе: подтверждение факта обработки, правовые основания и цели обработки, объем и категории обрабатываемых персональных данных, сроки хранения, сведения о лицах, которым данные могут быть переданы;

2. требовать уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав;

3. требовать перечень своих персональных данных, обрабатываемых Оператором, и источник их получения;

4. получать информацию о сроках обработки своих персональных данных, в том числе о сроках их хранения;

5. требовать извещения всех лиц, которым ранее были сообщены неверные или неполные его персональные данные, обо всех произведённых в них исключениях, исправлениях или дополнениях;

6. обжаловать в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке неправомерные действия или бездействие при обработке его персональных данных;

7. отозвать согласие на обработку персональных данных в порядке, предусмотренном разделом 7.3 настоящей Политики.

6.4. Субъект персональных данных обязан:

1. передавать достоверные, необходимые для достижения целей обработки персональные данные, а также подтверждать достоверность персональных данных предъявлением оригиналов документов;

2. в случае изменения персональных данных, необходимых для достижения целей обработки, сообщить Оператору уточнённые персональные данные и подтвердить изменения оригиналами документов;

3. выполнять требования законодательства Российской Федерации.

7. Порядок и условия обработки персональных данных

Оператор осуществляет как автоматизированную, так и неавтоматизированную обработку персональных данных.

Под обработкой персональных данных у Оператора понимается сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Оператор вправе передавать персональные данные органам дознания и следствия, иным уполномоченным органам по основаниям, предусмотренным действующим законодательством Российской Федерации.

Обработка персональных данных у Оператора производится на основе соблюдения принципов:

1. законности целей и способов обработки персональных данных;

2. соответствия целей обработки персональных данных целям, заранее определённым и заявленным при сборе персональных данных;

3. соответствия объёма и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных;

4. достоверности персональных данных, их достаточности для целей обработки, недопустимости обработки персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных;

5. недопустимости объединения созданных для несовместимых между собой целей баз данных, содержащих персональные данные;

6. хранения персональных данных в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки;

7. уничтожения по достижении целей обработки персональных данных или в случае утраты необходимости в их достижении.

Отказ соискателя, контрагента, работника, гражданина, подающего документы для получения визы или для легализации, от предоставления согласия на обработку его персональных данных влечёт за собой невозможность достижения целей обработки.

7.1. Передача персональных данных третьим лицам

Оператор передаёт персональные данные субъектов следующим категориям третьих лиц:

1. дипломатические представительства и консульские учреждения иностранных государств — для рассмотрения визовых заявлений и оформления виз;

2. компетентные органы иностранных государств — для легализации (апостиля, заверения) документов;

3. уполномоченные визовые сервисные центры и партнёры Оператора — на основании договоров и поручений на обработку персональных данных в соответствии со статьёй 6 Федерального закона № 152-ФЗ;

4. транспортные и курьерские службы — для доставки документов;

5. налоговые, правоохранительные и иные уполномоченные государственные органы Российской Федерации — по основаниям, предусмотренным законодательством.

Передача персональных данных третьим лицам осуществляется на основании договоров, заключённых между Оператором и получателем, либо на основании поручения на обработку персональных данных, с соблюдением требований статей 6 и 18 Федерального закона № 152-ФЗ.

7.2. Порядок ответа на запросы субъектов персональных данных

Оператор обязан сообщить субъекту персональных данных или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту, а также предоставить возможность ознакомления с этими персональными данными в течение 10 рабочих дней с даты получения запроса в соответствии со статьёй 20 Федерального закона № 152-ФЗ.

Указанный срок может быть продлён, но не более чем на 5 рабочих дней, с направлением субъекту персональных данных мотивированного уведомления.

Запрос направляется по контактными данным ответственного за организацию обработки персональных данных, указанным в разделе 1 настоящей Политики.

7.3. Порядок отзыва согласия на обработку персональных данных

Субъект персональных данных вправе отозвать своё согласие на обработку персональных данных путём направления Оператору письменного заявления по адресу места нахождения Оператора (115054, город Москва, Космодамианская набережная, дом 52 строение 7) или на адрес электронной почты ответственного за организацию обработки персональных данных (info.dme@blshelpline.com).

Заявление об отзыве согласия должно содержать:

1. фамилию, имя, отчество субъекта;

2. паспортные данные субъекта;

3. сведения, позволяющие идентифицировать субъекта в информационных системах Оператора (например, номер визовой заявки, номер телефона, адрес электронной почты, указанные при регистрации);

4. перечень персональных данных, обработку которых субъект просит прекратить (или указание на отзыв согласия в полном объёме);

5. дату составления и личную подпись (для заявления на бумажном носителе).

В случае отзыва согласия Оператор прекращает обработку персональных данных и уничтожает их в срок, не превышающий 30 дней с даты поступления заявления, если иное не предусмотрено законодательством Российской Федерации. Об уничтожении персональных данных Оператор уведомляет субъекта в течение 10 рабочих дней с даты уничтожения.

7.4. Трансграничная передача персональных данных

7.4.1. Оператор осуществляет трансграничную передачу персональных данных в целях оказания визовых и сопутствующих услуг, в том числе для передачи документов в консульские учреждения, посольства и визовые службы иностранных государств.

7.4.2. Трансграничная передача персональных данных осуществляется Оператором в соответствии со статьёй 12 Федерального закона № 152-ФЗ с учётом изменений, внесённых Федеральным законом от 26 июля 2026 года № 265-ФЗ «О внесении изменений в статью 12 Федерального закона "О персональных данных" и отдельные законодательные акты Российской Федерации».

7.4.3. В соответствии с Законом № 265-ФЗ участие иностранного государства в Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных не является самостоятельным основанием для признания этого государства обеспечивающим адекватную защиту прав субъектов персональных данных. Единственным критерием адекватности защиты является включение государства в перечень иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных, утверждаемый Роскомнадзором. При формировании перечня Роскомнадзор оценивает правовое регулирование в области персональных данных соответствующего государства и фактически применяемые им меры по обеспечению конфиденциальности и безопасности персональных данных.

7.4.4. Оператор перед осуществлением трансграничной передачи обязан проверить, включено ли государство, на территорию которого планируется передача, в действующий перечень Роскомнадзора. Оператор отслеживает актуальную версию перечня на официальном сайте Роскомнадзора.

7.4.5. До начала трансграничной передачи Оператор обязан направить в Роскомнадзор уведомление о намерении осуществлять трансграничную передачу персональных данных. Уведомление подаётся отдельно от уведомления об обработке персональных данных согласно статьи 22 Федерального закона № 152-ФЗ. В уведомлении указываются: правовое основание трансграничной передачи, цели передачи и дальнейшей обработки, категории передаваемых персональных данных, категории получателей, страны назначения, а также сведения о мерах по обеспечению безопасности персональных данных.

7.4.6. Если государство-получатель включено в перечень, Оператор вправе начать трансграничную передачу сразу после направления уведомления в Роскомнадзор, не дожидаясь истечения каких-либо сроков.

7.4.7. Если государство-получатель не включено в перечень, Оператор:

1. до подачи уведомления обязан получить от предполагаемого иностранного получателя персональных данных сведения о правовом регулировании в области персональных

данных в соответствующем государстве и о мерах, принимаемых получателем для обеспечения конфиденциальности и безопасности данных;

2. после подачи уведомления обязан воздержаться от трансграничной передачи до истечения 10 рабочих дней с даты поступления уведомления в Роскомнадзор. В течение этого срока Роскомнадзор вправе принять решение о запрете или об ограничении трансграничной передачи. Если по истечении 10 рабочих дней такое решение не принято, Оператор вправе начать передачу. При этом Роскомнадзор вправе запросить у Оператора дополнительные сведения. В этом случае срок рассмотрения приостанавливается до получения ответа. Оператор обязан ответить на запрос в течение 10 рабочих дней (с возможностью продления на 5 рабочих дней при направлении мотивированного уведомления).

7.4.8. Трансграничная передача персональных данных осуществляется при наличии согласия субъекта персональных данных на трансграничную передачу, если иное не предусмотрено законодательством. Согласие на трансграничную передачу не заменяет уведомление Роскомнадзора и не освобождает Оператора от соблюдения порядка, установленного статьёй 12 Федерального закона № 152-ФЗ.

7.4.9. Роскомнадзор вправе запретить или ограничить трансграничную передачу персональных данных для защиты конституционного строя, нравственности, здоровья, прав и законных интересов граждан, обеспечения обороны и безопасности государства. В случае получения запрета Оператор обязан обеспечить уничтожение персональных данных, ранее переданных иностранному получателю.

7.4.10. Оператор осуществляет регулярный мониторинг перечня Роскомнадзора на предмет изменения статуса государств-получателей. В случае исключения государства из перечня Оператор приостанавливает трансграничную передачу в такое государство и оценивает возможность продолжения передачи с учётом новых требований (получение сведений о правовом регулировании, режим ожидания 10 рабочих дней).

7.4.11. Трансграничная передача персональных данных не заменяет и не отменяет требование о локализации персональных данных граждан Российской Федерации в базах данных на территории России в соответствии со статьёй 18.5 Федерального закона № 152-ФЗ. Трансграничная передача может осуществляться параллельно с локализованной обработкой, но не допускает использование зарубежных баз данных в качестве основной системы хранения персональных данных граждан РФ.

8. Обеспечение безопасности персональных данных

Оператор предпринимает все необходимые правовые, организационные и технические меры для обеспечения безопасности персональных данных от неправомерного или случайного доступа, уничтожения, изменения, блокирования, копирования, предоставления, распространения и иных неправомерных действий.

Оператором для обеспечения безопасности персональных данных приняты следующие меры:

1. назначено лицо, ответственное за организацию обработки персональных данных;
2. назначен администратор безопасности информационной системы персональных данных;
3. утверждены документы, определяющие политику Оператора в отношении обработки персональных данных и устанавливающие процедуры, направленные на предотвращение и выявление нарушений законодательства. К таким документам, в частности, относятся: план мероприятий по обеспечению безопасности персональных данных в информационных системах персональных данных; перечень персональных данных, подлежащих защите; положение о разграничении прав доступа к персональным данным; приказ об утверждении перечня лиц,

допущенных к обработке персональных данных; положение о защите и обработке персональных данных; правила обработки персональных данных без использования средств автоматизации; приказ об утверждении мест хранения персональных данных и лиц, ответственных за соблюдение конфиденциальности персональных данных при их хранении; инструкция администратора безопасности информационных систем персональных данных; инструкция пользователя информационных систем персональных данных; инструкция ответственного за организацию обработки персональных данных; приказ о назначении группы реагирования на инциденты информационной безопасности;

4. устранение последствий нарушений законодательства Российской Федерации производится в соответствии с действующим законодательством, положением об обработке и защите персональных данных, а также инструкцией администратора безопасности персональных данных;

5. внутренний контроль соответствия обработки персональных данных законодательству Российской Федерации в данной сфере производится в соответствии с планом внутренних проверок, инструкцией администратора безопасности и положением об обработке и защите персональных данных;

6. для информационной системы персональных данных разработана модель угроз безопасности персональных данных, в которой при определении опасности угроз проводится оценка вреда, который может быть причинён субъектам персональных данных в случае нарушения законодательства;

7. для информационной системы персональных данных разработано техническое задание на создание системы защиты информации;

8. проведена оценка эффективности принимаемых мер по обеспечению безопасности персональных данных;

9. правила доступа к персональным данным утверждены в соответствующем положении, технически реализуются с помощью средств защиты информации;

10. сотрудники, допущенные к обработке персональных данных, проходят инструктажи по информационной безопасности, подписывают соглашение о неразглашении персональных данных, знакомятся с документами по защите персональных данных под роспись.

8.1. Порядок действий при обнаружении утечки персональных данных

8.1.1. Основание и определение инцидента

В соответствии с частью 3.1 статьи 21 Федерального закона № 152-ФЗ Оператор обязан уведомлять Роскомнадзор о фактах неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлёкшей нарушение прав субъектов персональных данных (далее — инцидент).

Под инцидентом понимается любое событие, в результате которого персональные данные стали доступны третьим лицам без согласия субъектов персональных данных, в том числе: несанкционированный доступ к базам данных, утечка данных через сеть Интернет, хищение носителей информации, ошибочная передача данных по незащищённым каналам связи, разглашение данных сотрудниками Оператора.

8.1.2. Первичное уведомление Роскомнадзора (в течение 24 часов)

При выявлении инцидента Оператор обязан в течение 24 часов с момента его обнаружения направить в Роскомнадзор первичное уведомление.

Уведомление направляется в электронном виде через форму на официальный электронный почтовый ящик Роскомнадзора с использованием усиленной квалифицированной

электронной подписи (УКЭП). Для подачи уведомления учётная запись на портале Госуслуг должна быть привязана к организации.

В первичном уведомлении указываются:

1. сведения об операторе: полное и сокращённое наименование, ИНН, ОГРН, адрес, адрес электронной почты;
2. дата и время выявления инцидента;
3. предполагаемые причины, повлекшие нарушение прав субъектов персональных данных;
4. характеристики затронутых персональных данных: категории субъектов, примерное количество записей в скомпрометированной базе, перечень категорий персональных данных, актуальность базы данных, период, в течение которого были собраны данные;
5. предполагаемый вред, нанесённый правам субъектов персональных данных;
6. принятые меры по устранению последствий инцидента;
7. ФИО и контактные данные лица, уполномоченного на взаимодействие с Роскомнадзором по инциденту;
8. иные сведения (при наличии), включая источник получения информации об инциденте.

8.1.3. Внутреннее расследование

Параллельно с направлением первичного уведомления Оператор инициирует внутреннее расследование инцидента. Для проведения расследования приказом Оператора создаётся рабочая группа в составе:

- ответственного за организацию обработки персональных данных;
- администратора безопасности информационной системы персональных данных;
- IT-специалиста;
- юриста;
- иных сотрудников по усмотрению руководства.

Внутреннее расследование включает:

1. установление причин и обстоятельств инцидента;
2. определение объёма скомпрометированных персональных данных и количества затронутых субъектов;
3. выявление лиц, действия которых стали причиной инцидента;
4. оценку вреда, нанесённого субъектам персональных данных;
5. разработку мер по устранению последствий и предотвращению аналогичных инцидентов.

8.1.4. Дополнительное уведомление Роскомнадзора (в течение 72 часов)

В течение 72 часов с момента выявления инцидента Оператор обязан направить в Роскомнадзор дополнительное уведомление с результатами внутреннего расследования.

Дополнительное уведомление направляется тем же способом (через портал персональных данных Роскомнадзора) с указанием номера и ключа первичного уведомления.

В дополнительном уведомлении указываются:

1. результаты внутреннего расследования: уточнённые причины инцидента, оценённый вред, нанесённый субъектам персональных данных;
2. сведения о лицах, действия которых стали причиной инцидента (ФИО и должность сотрудника Оператора либо ФИО, наименование, IP-адрес, предполагаемое местонахождение стороннего виновника — при наличии такой информации);
3. сведения об информационной системе, в которой произошёл инцидент;

4. дополнительно принятые меры по устранению последствий инцидента и предотвращению повторения;

5. реквизиты решения (приказа) Оператора о проведении внутреннего расследования.

Если на момент истечения 72 часов расследование не завершено, Оператор направляет доступные сведения в имеющемся объеме и продолжает информировать Роскомнадзор по мере поступления новой информации.

8.1.5. Уведомление субъектов персональных данных

Хотя статья 21 Федерального закона № 152-ФЗ прямо не обязывает Оператора уведомлять субъектов об инциденте, Оператор в целях защиты прав субъектов персональных данных принимает на себя обязательство уведомлять субъектов, чьи данные были затронуты инцидентом, в течение 5 рабочих дней с момента завершения внутреннего расследования.

Уведомление субъекта включает:

1. описание характера инцидента и категорий затронутых персональных данных;
2. дату инцидента и дату его обнаружения;
3. оценку возможных последствий для субъекта;
4. перечень мер, принятых Оператором для устранения последствий;
5. рекомендации субъекту по самостоятельной защите (смена паролей, мониторинг транзакций, обращение в правоохранительные органы при необходимости);
6. контактные данные для получения дополнительной информации.

Уведомление направляется по адресу электронной почты субъекта (при наличии) или по почтовому адресу. При массовом инциденте с неполными контактами Оператор вправе разместить публичное уведомление на официальном сайте.

8.1.6. Дополнительные уведомления

Если инцидент произошёл в сети Интернет или с удалённого сервера, Оператор дополнительно уведомляет Государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА) через соответствующее подразделение (при подключении к инфраструктуре ГосСОПКА — через её систему; в остальных случаях — по телефону или электронной почте).

8.1.7. Фиксация и хранение

Все действия, связанные с выявлением, расследованием и уведомлением об инциденте, фиксируются в журнале регистрации инцидентов информационной безопасности. Каждое уведомление, направленное в Роскомнадзор, сохраняется с указанием даты, времени, номера и ключа уведомления. Акт внутреннего расследования хранится не менее 5 лет.

8.1.8. Ответственность

Непредставление или несвоевременное представление уведомлений в Роскомнадзор влечёт административную ответственность по статье 13.11 КоАП РФ. За не уведомление об утечке штраф для юридических лиц составляет от 1 млн. до 3 млн. рублей. За саму утечку данных штрафы зависят от количества пострадавших субъектов: от 3 млн. до 5 млн. рублей (1 тыс. – 10 тыс. субъектов), от 10 млн. до 15 млн. рублей (более 100 тыс. субъектов), от 15 млн. до 20 млн. рублей при утечке биометрических данных. При повторной утечке применяются оборотные штрафы — от 1% до 3% годовой выручки, но не менее 20 млн. и не более 500 млн. рублей.

9. Заключительные положения

К настоящей Политике обеспечивается неограниченный доступ. Политика размещается на официальном сайте Оператора.

Настоящая Политика подлежит изменению и дополнению в случае появления новых законодательных актов и специальных нормативных документов по обработке и защите персональных данных, а также в случае изменения структуры и целей обработки персональных данных Оператором. Политика пересматривается не реже одного раза в три года.

Контроль исполнения требований настоящей Политики осуществляется ответственным за организацию обработки персональных данных Оператора.

Согласие на обработку персональных данных оформляется отдельно от ознакомления с настоящей Политикой. Согласие должно быть конкретным, предметным, информированным, сознательным и однозначным. Автоматически проставляемые отметки о согласии не допускаются — субъект персональных данных должен совершить самостоятельное активное действие для выражения согласия (отдельная подпись, отдельная форма согласия, проставление отметки в визуальном обособленном блоке).

9.1. Использование файлов cookie

Оператор с целью улучшения использования и просмотра веб-страниц субъектом персональных данных использует файлы небольшого размера (cookie-файлы), создаваемые устройством (компьютером, смартфоном, планшетом или другим электронным устройством, предназначенным для просмотра информации на веб-странице) в момент, когда субъект персональных данных заходит на сайт Оператора.

Оператор использует следующие типы cookie-файлов:

1. технические (функциональные) — обеспечивают корректную работу сайта, сохранение настроек пользовательского интерфейса, идентификацию сессии. Хранятся до 1 года;
2. аналитические — собирают агрегированную статистику посещений для улучшения работы сайта. Хранятся до 14 месяцев;
3. сервисные — обеспечивают работу сторонних виджетов и интеграций (например, карты, формы записи). Хранятся до окончания сессии.

Субъект персональных данных может разрешать, блокировать или удалять cookie-файлы, установленные на его устройстве, через конфигурацию параметров в своём интернет-браузере. В случае запрета использования cookie-файлов субъект персональных данных может утратить доступ к некоторым функциям веб-сайта Оператора.

Оператор не использует cookie-файлы для распространения рекламных материалов третьих лиц.

9.2. Иные положения

В соответствии с законодательными и нормативными требованиями Оператор вправе изменить условия настоящей Политики в одностороннем порядке с обязательным размещением обновлённой редакции на сайте Оператора. Изменения вступают в силу с момента размещения обновлённой редакции, за исключением случаев изменения законодательства Российской Федерации, когда новые требования вступают в силу в соответствии с законодательством.

Оператор сохраняет конфиденциальность в отношении сведений, полученных в процессе работы. Оператор не несёт ответственности за персональные данные субъекта, самостоятельно размещённые субъектом в общедоступных источниках информации.



Ответственность должностных лиц Оператора, имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных, определяется в соответствии с законодательством Российской Федерации и внутренними документами Оператора.