KONSU
SINCE 1993
30 YEARS

Персональные данные – основные практики с учетом изменений 2023

Анна Резникова
Руководитель практики трудового и миграционного права

СОДЕРЖАНИЕ

1. Обработка персональных данных в 2023

2. Уничтожение персональных данных: новые правила

3. Оценка степени вреда при нарушении закона о персональных данных: новый порядок

4. Особенности передачи персональных данных за рубеж 2023

5. Ужесточение проверок Роскомнадзора при работе операторов с персональными данными

6. Документы, которые необходимо иметь операторам по персональным данным в 2023

1. ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ В 2023

С 1 марта 2023 года – множество изменений в части работы с персональными данными, которые затрагивают различные сферы как бизнеса, так и обычных физических лиц.

Персональные данные – любая информация, прямо или косвенно относящаяся к субъекту персональных данных – определенному или определяемому физическому лицу.

Обработка персональных данных – действие или совокупность действий, которые совершают с персональными данными сотрудника. Например, когда компания собирает и записывает ПД соискателя, чтобы заполнить трудовой договор при трудоустройстве. Также, если компания – владелец интернет-сайта и собирает данные посетителей через специальную форму, она тоже занимается обработкой ПД.

1. ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ В 2023

На заметку: еще до 1 марта 2023 года работодатели обязаны были передавать РКН специальные уведомления об обработке персональных данных. С 1 марта 2023 года требований к обработке персональных данных становится еще больше. Кроме того, в 2023 году РКН усилит проверки за персональными данными. В частности, начнет проводить “дистанционные” проверки операторов персональных данных.

Уведомление об изменении персональных данных: новый срок

С 1 марта будет больше времени, чтобы известить РКН об изменении ПД. Если сведения, которые указали в уведомлении, изменились, об этом нужно сообщить в РКН не позднее 15-го числа месяца, следующего за месяцем, в котором произошли изменения.

До 1 марта такое уведомление направлялось в течение 10 рабочих дней с момента изменений. Уведомление подается по форме из приложения № 2 к приказу Роскомнадзора от 28.10.2022 № 180.

2. УНИЧТОЖЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

С 1 марта нужно фиксировать факт уничтожения персональных данных актом по новой форме. Раньше оформить акт об уничтожении можно было в свободной форме, а теперь необходимо включить в него 10 обязательных видов данных. **Основание: Приказ Роскомнадзора от 28.10.2022 N 179.**

С 1 марта 2023 года работодатель должен фиксировать, что уничтожил ПД, двумя документами:

- ✓ актом об уничтожении персональных данных;
- ✓ выгрузкой из журнала регистрации событий в информационной системе персональных данных.

Сам процесс должен проводиться специальной комиссией, созданной как раз для подобных случаев. После завершения процедуры создается акт, подписываемый членами комиссии и руководителем.

2. УНИЧТОЖЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

В случае, если обработка ПД осуществляется оператором **без использования средств автоматизации**, подтверждающим документом является акт об уничтожении персональных данных.

В случае, если обработка персональных данных осуществляется оператором **с использованием средств автоматизации**, подтверждающими документами являются акт и выгрузка из журнала регистрации событий в информационной системе персональных данных.

Акт в электронной форме признается электронным документом, равнозначным акту на бумажном носителе. Поскольку в приказе РКН не уточняется, какая именно электронная подпись должна применяться, акт следует подписывать усиленной квалифицированной электронной подписью, если локальными нормативными актами оператора персональных данных не предусмотрено, что он может быть подписан усиленной неквалифицированной электронной подписью.

В случае, если обработка персональных данных осуществляется оператором **одновременно с использованием средств автоматизации и без использования средств автоматизации**, подтверждающими документами являются акт и выгрузка из журнала.

2. УНИЧТОЖЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

Наказание за отсутствие акта:

Если проверяющие не обнаружат акт при проверке, посчитают невыполненными требования об обязательном уничтожении персональных данных и накажут – штраф:

- на директора составит от 8 000 руб. до 20 000 руб.;
- на ИП от 20 000 до 40 000 руб.;
- на юридическое лицо: от 50 000 руб. до 90 000 руб. *(ч. 5 ст. 13.11 КоАП РФ).*

Повторное аналогичное нарушение способно серьезно истощить «карман» оператора ПД *(ч. 5.1 ст. 13.11 КоАП РФ)*:

- должностное лицо от 30 000 до 50 000 руб.;
- ИП от 50 000 до 100 000 руб.;
- юридическое лицо от 300 000 до 500 000 руб.

2. УНИЧТОЖЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

Обязательные реквизиты акта об уничтожении ПД:

- наименование компании или ФИО (при наличии) физического лица – оператора ПД;
- адрес оператора ПД;
- наименование компании или ФИО (при наличии) физического лица, кто обрабатывал ПД по поручению оператора (при наличии такого поручения);
- ФИО (при наличии) субъектов ПД или иная информация, относящаяся к определенным физическим лицам, чьи персональные данные были уничтожены;
- ФИО (при наличии) и должность лиц, уничтоживших ПД и их подписи;
- перечень категорий уничтоженных ПД;
- наименование уничтоженных материальных носителей с ПД с указанием количества листов в отношении каждого такого носителя (если ПД обрабатывались без использования средств автоматизации – на бумаге);
- наименование информационной системы ПД, из которой были уничтожены ПД (если ПД обрабатывались с использованием средств автоматизации);
- способ уничтожения ПД;
- причина уничтожения ПД;
- дата уничтожения ПД.

2. УНИЧТОЖЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

Выгрузка из журнала должна содержать:

- ФИО (при наличии) субъектов ПД или иную информацию, относящуюся к определенным физическим лицам, чьи ПД были уничтожены;
- перечень категорий уничтоженных ПД;
- наименование информационной системы ПД, из которой они были уничтожены;
- причина уничтожения ПД;
- дата уничтожения ПД.

При невозможности указать в выгрузке из журнала какие-либо сведения, их следует отразить в акте об уничтожении ПД.

Хранить все документы об уничтожении ПД следует не менее 3 лет с момента уничтожения. Как именно исчислять срок, в документе не уточняется. Рекомендуем хранить документы с небольшим запасом по времени.

3. ОЦЕНКА СТЕПЕНИ ВРЕДА ПРИ НАРУШЕНИИ ЗАКОНА О ПЕРСОНАЛЬНЫХ ДАННЫХ

С 1 марта 2023 года нужно оценивать степень вреда, который возникает, если нарушен закон о ПД.

Ущерб для персональных данных – моральный или материальный ущерб субъекту ПД, который реально причинен или существует угроза его причинения при нарушении оператором положений Федерального закона № 152-ФЗ от 27.07.2006.

Каждая компания обязана проводить оценку потенциального вреда субъектам персональных данных и реализовывать комплекс мер, направленных на обеспечение безопасности и охраны ПД, недопущение причинения ущерба.

РКН утвердил специальные правила, по которым работодатели должны оценивать вред, который может возникнуть, если будут нарушены правила обработки ПД *(приказ Роскомнадзора от 27.10.2022 № 178).*

Действие приказа ограничено во времени – он действует до 1 марта 2029 года.

3. ОЦЕНКА СТЕПЕНИ ВРЕДА ПРИ НАРУШЕНИИ ЗАКОНА О ПЕРСОНАЛЬНЫХ ДАННЫХ

Приказ № 178 от 27.10.2022 выделяет 3 степени (п. 2.1-2.3 приказа):

- высокая;
- средняя;
- низкая.

Акт оценки потенциального вреда субъектам ПД предназначен для оформления результаты оценки вреда, который может быть причинен субъектам ПД в случае нарушения требований законодательства о ПД.

Все акты готовятся и подписываются членами комиссии, которыми могут быть лица, имеющие доступ к персональным данным работников.

Если физическому лицу могут причинить вред разных степеней, надо учитывать более высокую из них.

3. ОЦЕНКА СТЕПЕНИ ВРЕДА ПРИ НАРУШЕНИИ ЗАКОНА О ПЕРСОНАЛЬНЫХ ДАННЫХ

Какие ПД к какой степени вреда относятся:

Степень вреда	Как и какие ПД обрабатываются в компании
Высокая	**1. Биометрические ПД:** ▪ Фотографическое изображение человека; ▪ Видеоизображение человека; ▪ Дактилоскопические данные; ▪ Информация о радужной оболочке глаза; ▪ Результаты анализов ДНК; ▪ Данные о голосе. На заметку: Если фото используется для установления личности человека, оно признается биометрическими ПД. Например, к биометрическим ПД относят фото на пропуск, поскольку сравнивая фото с лицом предъявителя пропуска, компания можете установить его личность. *(ч. 1 ст. 11 Закона о персональных данных, Письмо Минцифры России от 17.07.2020 N ОП-П24-070-19433)*
	2. Специальные категории ПД, в т.ч. сведения о состоянии здоровья и судимости.
	3. ПД несовершеннолетних
	4. Поручаете иностранному гражданину или компании обработку ПД
	5. Собираете ПД с использованием баз, которые находятся за пределами РФ

3. ОЦЕНКА СТЕПЕНИ ВРЕДА ПРИ НАРУШЕНИИ ЗАКОНА О ПЕРСОНАЛЬНЫХ ДАННЫХ

Какие ПД к какой степени вреда относятся:

Степень вреда	Как и какие ПД обрабатываются в компании
Средняя	1. Распространение ПД на официальном сайте – предоставление данных неограниченному кругу лиц
	2. Обработка ПД в дополнительных целях, которые отличаются от первоначальной цели сбора ПД
	3. Потенциальным клиентам напрямую предлагаются товары и услуги, для чего используются базы другого оператора
	4. Согласие на обработку ПД взято на официальном интернет-сайте без дальнейшей проверки субъекта ПД

Степень вреда	Как и какие ПД обрабатываются в компании
Низкая	1. Ведение общедоступных источников ПД (в т.ч. справочники, адресные книги) *ст. 8 № 152-ФЗ от 27.07.2006*
	2. Назначение в качестве ответственного за обработку ПД – лица, с которым не заключен трудовой договор

4. ОСОБЕННОСТИ ПЕРЕДАЧИ ПЕРСОНАЛЬНЫХ ДАННЫХ ЗА РУБЕЖ 2023

С 1 марта 2023 года компании должны будут уведомлять Роскомнадзор о зарубежных поставщиках, которые получают доступ к личным данным россиян *(ст. 12 Закона № 152ФЗ).* РКН примет решение, можно ли передавать данные этим контрагентам или нельзя. О своем решении компанию уведомят в течение 10 рабочих дней.

Новшество напрямую касается онлайн-продавцов. Разрешение не выдадут, если иностранный контрагент работает в стране, которая с точки зрения РКН не обеспечивает защиту данных. Если поставщик находится в стране, которая ратифицировала Конвенцию Совета Европы о защите физлиц при автоматизированной обработке персональных данных, разрешение с большей вероятностью дадут. Конвенцию, к примеру, ратифицировали Армения, Азербайджан, Сербия, Турция.

Уведомление о намерении осуществлять трансграничную передачу можно будет оформить на бумаге или в электронном виде. Подавать его нужно будет отдельным документом, а не вместе с общим уведомлением о намерении осуществлять обработку персональных данных. Для подачи сведений на сайте РКН сделали специальный раздел – **https://pd.rkn.gov.ru/cross-border-transmission/form/**

4. ОСОБЕННОСТИ ПЕРЕДАЧИ ПЕРСОНАЛЬНЫХ ДАННЫХ ЗА РУБЕЖ 2023

На заметку: Операторам, которые уведомили РКН о трансграничной передаче до 01.03.2023, не нужно подавать новое уведомление после 1 марта – но только пока в их работе не произойдут изменения, которые предполагают создание новых трансграничных потоков – в новые страны или для новых целей.

После отправки уведомления о трансграничной передаче – оператор сможет передавать информацию в страны, которые участвуют в Конвенции Совета Европы о защите физлиц при автоматизированной обработке ПД или включены в Перечень иностранных государств, обеспечивающих защиту данных *(ч. 10, 11 ст. 12 №152-ФЗ)*.

Это можно делать до тех пор, пока РКН не примет решение о запрете или ограничении передачи. Если страна не обеспечивает адекватный уровень защиты ПД, оператору нельзя передавать сведения в течение 10 рабочих дней после подачи уведомления.

Важно: Если трансграничная передача необходима для защиты жизни, здоровья или других жизненно важных целей, можно отправлять ПД, не дожидаясь решения РКН.

Решение о запрете или ограничении РКН принимает после рассмотрения уведомления *(Постановление Правительства №24 от 16.01.2023)*. Если передачу ограничат или запретят, оператор должен проконтролировать, чтобы иностранные лица уничтожили полученную информацию.

5. УЖЕСТОЧЕНИЕ ПРОВЕРОК РОСКОМНАДЗОРА ПРИ РАБОТЕ ОПЕРАТОРОВ С ПЕРСОНАЛЬНЫМИ ДАННЫМИ

За нарушение работы с ПД в 2023 году РКН будет привлекать к ответственности чаще – причем для этого не всегда потребуется проводить выездные проверки *(письмо Роскомнадзора от 31.01.2023 № 09-6488)*.

Внеплановых проверок будет больше. Правительство расширило список оснований для внеплановых проверок по персональным данным *(Постановление от 04.02.2023 № 161).*

Например, по решению главы или замглавы РКН в компанию, в т.ч. аккредитованную IT-организацию, могут прийти с внеплановой проверкой, если выявят факт распространения в интернете баз с ПД.

5. УЖЕСТОЧЕНИЕ ПРОВЕРОК РОСКОМНАДЗОРА ПРИ РАБОТЕ ОПЕРАТОРОВ С ПЕРСОНАЛЬНЫМИ ДАННЫМИ

Наказать могут и без выезда в компанию. В некоторых ситуациях зафиксировать правонарушение в сфере ПД и привлечь к ответственности могут даже без выездных контрольных мероприятий *(письмо Роскомнадзора от 31.01.2023 № 09-6488).*

Речь идет о нарушениях, которые оговорены в частях 1–2.1 и 4 статьи 13.11 КоАП. Например, к особым нарушениям причислена обработка данных без письменного согласия, а также обработка, несовместимая с целями сбора данных.

РКН уточняет в своих разъяснениях, что по таким нарушениям контролеры могут действовать «бесконтактно» (без взаимодействия с нарушителем). Например, если нарушение обнаружил сам сотрудник Роскомнадзора и у него есть полномочия составлять протокол или поступило указание от прокуратуры.

Поводом для возбуждения дела могут послужить жалоба, сообщения в СМИ, например, об утечке данных *(п. 1–3 ч. 1 ст. 28.1 КоАП).*

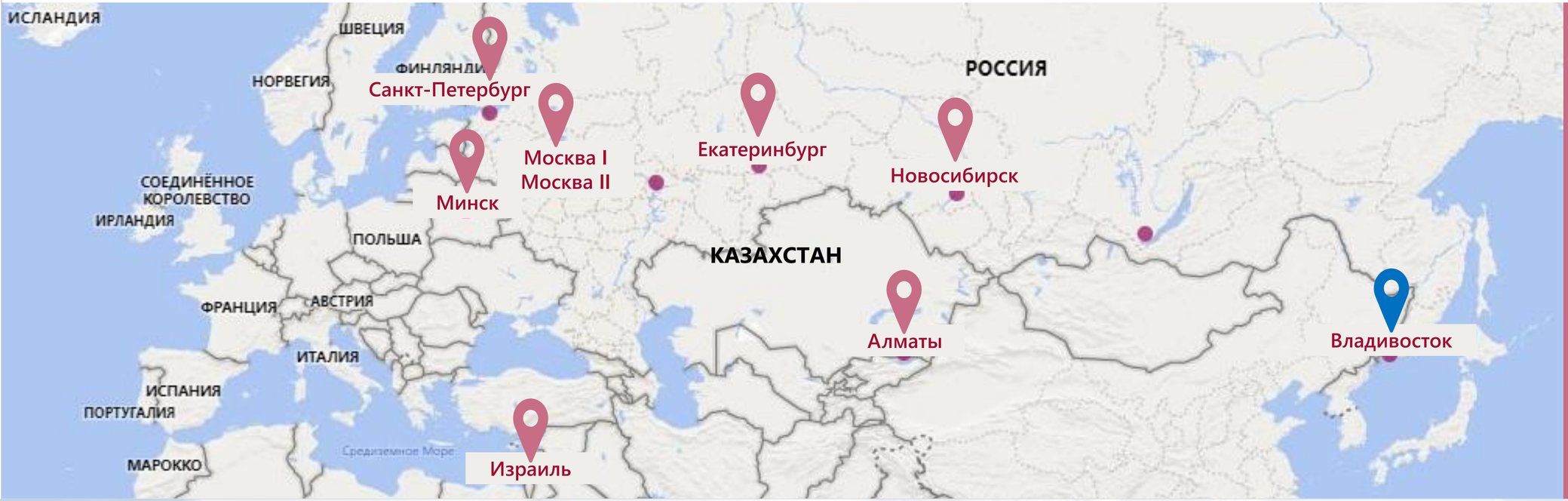
6. ДОКУМЕНТЫ, КОТОРЫЕ НЕОБХОДИМО ИМЕТЬ ОПЕРАТОРАМ ПО ПЕРСОНАЛЬНЫМ ДАННЫМ В 2023

- Положение о работе с персональными данными работников, а также клиентов, контрагентов, соискателей;
- Согласие на обработку персональных данных работника;
- Журналы учета персональных данных (журнал учета внутреннего доступа к ПД, журнал проверок наличия документов, содержащих ПД работника, журнал учета выдачи ПД работников организациям и государственным органам);
- Обязательство о неразглашении ПД работниками, имеющими доступ к этим данным;
- Приказ о назначении ответственного за обеспечение безопасности ПД;
- Приказ об установлении списка лиц, имеющих доступ к ПД работников;
- Согласие на обработку персональных данных соискателя, клиента, контрагента;
- Согласие на обработку персональных данных, разрешенных субъектом на распространение;
- Форма требование о прекращении передачи (распространения, предоставления, доступа) ПД, разрешенных субъектом персональных данных для распространения
- Отзыв согласия на обработку ПД.

6. ДОКУМЕНТЫ, КОТОРЫЕ НЕОБХОДИМО ИМЕТЬ ОПЕРАТОРАМ ПО ПЕРСОНАЛЬНЫМ ДАННЫМ В 2023

- Форма запроса субъекта персональных данных на уточнение персональных данных;
- Форма запроса субъекта персональных данных на блокирование персональных данных;
- Разъяснение юридических последствий отказа предоставить персональные данные;
- Акт об уничтожении персональных данных, выгрузка из журнала регистрации событий в информационной системе персональных данных (новые требования);
- Акт определения уровня защищенности персональных данных (разрабатывается совместно с IT-специалистами);
- Акт оценки возможного вреда субъектам персональных данных (разрабатывается совместно с IT-специалистами);
- Политика защиты и обработки персональных данных размещается на сайте компании, если она обрабатывает ПД физических лиц.

SOFTLINE CLOUD – МУЛЬТИОБЛАЧНАЯ ПЛАТФОРМА С ФАНАТИЧНОЙ СЕРВИСНОЙ ПОДДЕРЖКОЙ С УПОРОМ НА ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ



9

дата-центров:

Москва x 2,
Санкт-Петербург,
Новосибирск,
Екатеринбург,
Алматы (Казахстан),
Минск,
Израиль,
Владивосток

Решения для бизнеса

Виртуальный офис • САПР в облаке • Корпоративная почта • Виртуальный рабочий стол • DRaaS

Аренда виртуальных мощностей

Виртуальная инфраструктура • Виртуальные серверы • Виртуальный ЦОД • Частное облако • Резервное копирование в облаке

Аренда оборудования

Dedicated-серверы • Colocation: размещение оборудования в дата-центре • HaaS / DaaS

Облачные платформы

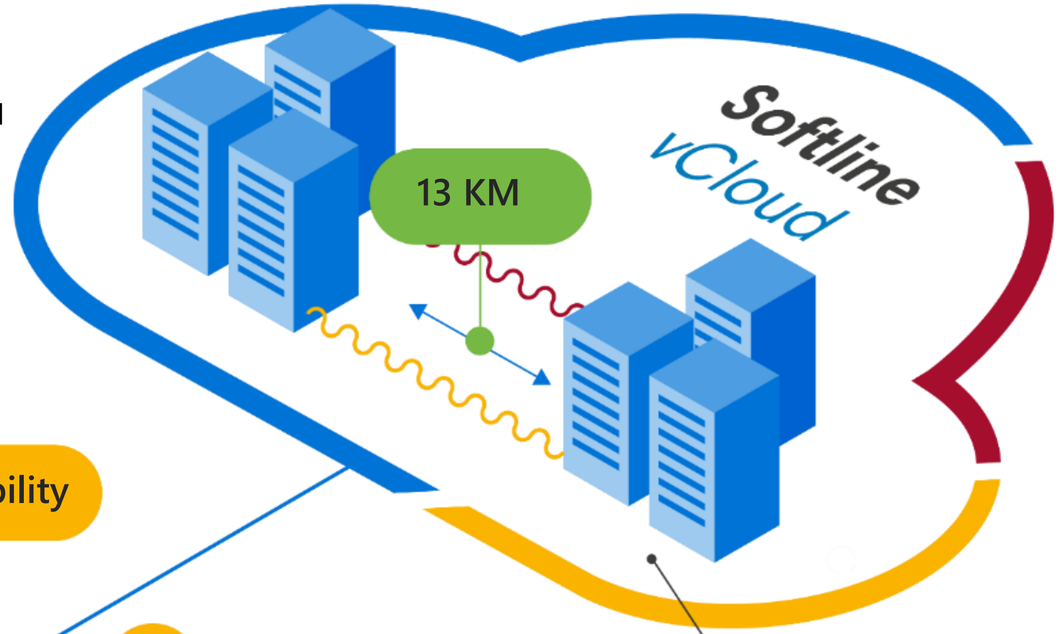
Softline Cloud • Private Cloud • Any / MultiCloud • Active Platform • CloudMaster

ПУБЛИЧНОЕ ОБЛАКО SOFTLINE CLOUD

Защищенное облако Softline, соответствующее требованиями к защите персональных данных уровня защищенности **152 ФЗ УЗ 3 и 4, сертификат PCI DSS, ISO 27001/27017/27018**

Платформа виртуализации с удобным интерфейсом управления виртуальными ресурсами

SLA 99,982%
Круглосуточная техническая поддержка 24x7x365



Cloud Availability

Инфраструктура заказчика

Подключение **L2**, L3

CPU 2.2 - **2.6 GHz** – стандарт
> 3.0 GHz – для приложений типа ERP, **1C DB**

Размещение в **ЦОД** уровня **Tier III**:

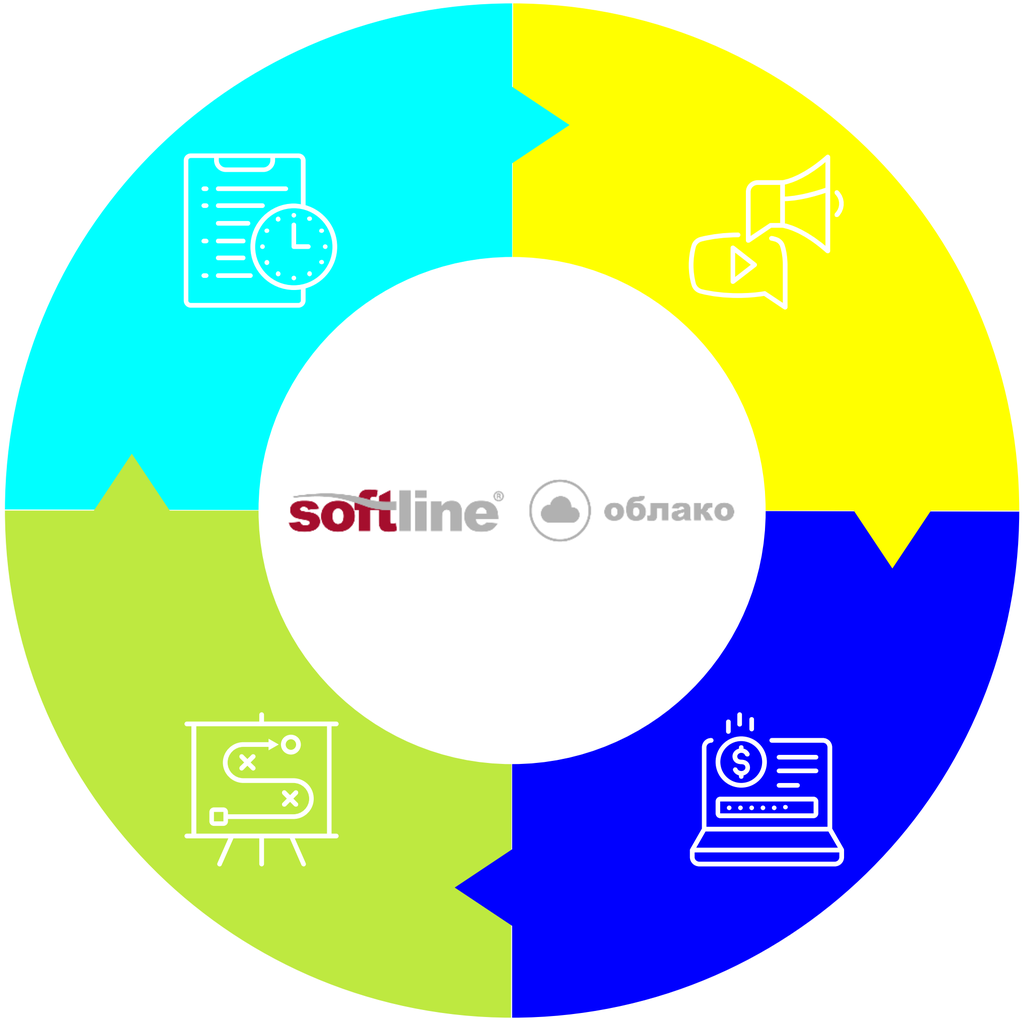
1. **Москва I**
2. **Москва II**
3. **Санкт-Петербург**
4. **Екатеринбург**
5. **Новосибирск**
6. **Казахстан**
7. **Израиль (Нетания)**
8. **Иркутск**
9. **Минск**
10. **Казань**
11. **Владивосток**

ЕДИНАЯ ЭКОСИСТЕМА СЕРВИСОВ SOFTLINE

ИНТЕГРАЦИОННЫЕ РЕШЕНИЯ SOFTLINE

СЛОЖНЫЕ ПРОЕКТЫ ПО МИГРАЦИИ В ОБЛАКО

ПРОЕКТЫ ПО РАЗВИТИЮ ЛОКАЛЬНОЙ ИНФРАСТРУКТУРЫ



ТЕХНИЧЕСКАЯ ПОДДЕРЖКА SOFTLINE

БАЗОВАЯ ПОДДЕРЖКА ЛОКАЛЬНОЙ ИНФРАСТРУКТУРЫ (ЗИП, ОБНОВЛЕНИЯ)

ПРЕМЬЕР ПОДДЕРЖКА (MICROSOFT, ORACLE, REDHAT, CITRIX)

ОПТИМИЗАЦИЯ И РАЗВИТИЕ

ДОРОЖНАЯ КАРТА ПЕРЕХОДА В ОБЛАКО

ДОРОЖНАЯ КАРТА ПЕРЕХОДА НА РОССИЙСКИЕ РЕШЕНИЯ

ОПТИМИЗАЦИЯ СТОИМОСТИ ОБЛАКОВ

ЗАЩИТА ОТ КИБЕРУГРОЗ

ВЫСШИЕ СТАТУСЫ ЗАЩИТЫ ДАННЫХ В ОБЛАКЕ SOFTLINE

ЭКОСИСТЕМА СЕРВИСОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ SOFTLINE

СПАСИБО
ЗА ВНИМАНИЕ!

115114 Москва
1-й Дербеневский пер. 5
+7 495 788 00 05
konsugroup.com
info@konsugroup.com

196006 Санкт-Петербург
Лиговский проспект 266
+7 812 325 82 94

050010/A25D9D1 Алматы
пр. Достык 38

00210 Хельсинки
Италахденкату 15-17