**«ИГРА В КАДРЫ»**

Задание № 8



Общее задание предлагается рассмотреть комплексно посредством выделения отдельных подзадач:

1. ПДн – понятие и действия, которые с ними производятся.
2. Понятие локализации ПДн
3. Решения, применяемые в SAP для защиты ПДн.
4. Трансграничная передача ПДн.
5. Особенности получения и обработки ПДн на территории России кандидатов на вакантные должности.
6. Краткий алгоритм действий по работе с персональными данными кандидатов на вакантные должности.
7. **Персональные данные (далее –ПДн) –**

**понятия и действия, которые с ними производятся**

Понятийный аппарат «ПДн» определяется Федеральным законом от 26 июля 2006г. № 152 - ФЗ «О ПДн» (далее – 152-ФЗ).

* 1. **ПДн (п.1.ст.3 152-ФЗ)**

В соответствии с [п. 1 ст. 3](http://www.consultant.ru/document/cons_doc_LAW_61801/4f41fe599ce341751e4e34dc50a4b676674c1416/)  ***ПДн*** *(далее – ПДн)* *- любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту ПДн);*

*Текущая судебная практика в большей степени склоняется к ограничительному толкованию рассматриваемого понятия и придерживается той позиции, что ПДн – это лишь те данные, которые позволяют идентифицировать конкретного гражданина.*

В соответствии с [п. 2 ст. 3](http://www.consultant.ru/document/cons_doc_LAW_61801/4f41fe599ce341751e4e34dc50a4b676674c1416/) 152 - ФЗ:

**1.2. Оператор ПДн (п.2.ст.3 152-ФЗ)**

***Оператор*** *- государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку ПДн, а также определяющие цели обработки ПДн, состав ПДн, подлежащих обработке, действия (операции), совершаемые с персональными данным.*

*При решении кейса под операторами предлагается понимать сотрудников службы управления персоналом, руководителей Департамента либо глобального HR, всех, кто будет работать с резюме(анкетами) кандидатов на вакантные должности.*

**1.3. Понятие обработки ПДн (пп.3-11 ст.3 152-ФЗ)**

***Обработка ПДн*** *- любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение ПДн.*

***автоматизированная обработка ПДн*** *- обработка ПДн с помощью средств вычислительной техники;*

***распространение ПДн*** *- действия, направленные на раскрытие ПДн неопределенному кругу лиц;*

***предоставление ПДн*** *- действия, направленные на раскрытие ПДн определенному лицу или определенному кругу лиц;*

***блокирование ПДн*** *- временное прекращение обработки ПДн (за исключением случаев, если обработка необходима для уточнения ПДн);*

***уничтожение ПДн*** *- действия, в результате которых становится невозможным восстановить содержание ПДн в информационной системе ПДн и (или) в результате которых уничтожаются материальные носители ПДн;*

***обезличивание ПДн*** *- действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность ПДн конкретному субъекту ПДн;*

***информационная система ПДн*** *- совокупность содержащихся в базах данных ПДн и обеспечивающих их обработку информационных технологий и технических средств;*

***трансграничная передача ПДн*** *- передача ПДн на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.*

**1.4. Принципы обработки ПДн (ст. 5 152-ФЗ)**

*1. Обработка ПДн должна осуществляться на законной и справедливой основе.*

*2. Обработка ПДн должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка ПДн, несовместимая с целями сбора ПДн.*

*3. Не допускается объединение баз данных, содержащих ПДн, обработка которых осуществляется в целях, несовместимых между собой.*

*4. Обработке подлежат только ПДн, которые отвечают целям их обработки.*

*5. Содержание и объем обрабатываемых ПДн должны соответствовать заявленным целям обработки. Обрабатываемые ПДн не должны быть избыточными по отношению к заявленным целям их обработки.*

*6. При обработке ПДн должны быть обеспечены точность ПДн, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки ПДн. Оператор должен принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных.*

*7. Хранение ПДн должно осуществляться в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели обработки ПДн, если срок хранения ПДн не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн. Обрабатываемые ПДн подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.*

**1.5. Условия обработки ПДн (ст. 6 152-ФЗ)**

В соответствии с [п. 1 ч. 1 ст. 6](consultantplus://offline/ref=DDB676B58918430638255AEFE3F3F95E12E2CB68BC0F1515BBDE878C4FEE068B9622425ED04E05A24E0040D2857F7FE0112B956D33E7D604o3Z3R) Федерального закона "О ПДн" **обработка ПДн осуществляется оператором с согласия субъектов ПДн**, за исключением случаев, предусмотренных [п. 2](consultantplus://offline/ref=DDB676B58918430638255AEFE3F3F95E12E2CB68BC0F1515BBDE878C4FEE068B9622425ED04E05A1470040D2857F7FE0112B956D33E7D604o3Z3R) - [11 ч. 1 указанной статьи](consultantplus://offline/ref=DDB676B58918430638255AEFE3F3F95E12E2CB68BC0F1515BBDE878C4FEE068B9622425ED04E05A14E0040D2857F7FE0112B956D33E7D604o3Z3R).

В частности для решения нашего кейса необходимо учитывать, что не требуется согласия на обработку ПДн при осуществлении обработки ПДн в случае, когда доступа неограниченного круга лиц к ПДн, предоставлен непосредственно субъектом ПДн либо по его просьбе. (Например, размещение резюме кандидата в кадровом агентстве или в Интернете).

Также при работе с ПДн оператор обязан соблюдать принципы и правила обработки ПДн, предусмотренные 152-ФЗ, в том числе соблюдать конфиденциальность ПДн и обеспечивать безопасность ПДн при их обработке, (требования к защите обрабатываемых ПДн)

Согласно [ч. 3 ст. 6](consultantplus://offline/ref=DDB676B58918430638255AEFE3F3F95E12E2CB68BC0F1515BBDE878C4FEE068B9622425ED04E05A0460040D2857F7FE0112B956D33E7D604o3Z3R) 152-ФЗ оператор вправе поручить обработку ПДн другому лицу с согласия субъекта ПДн, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора.

В соответствии с [ч. 4. ст. 6](consultantplus://offline/ref=DDB676B58918430638255AEFE3F3F95E12E2CB68BC0F1515BBDE878C4FEE068B9622425ED04E05A0450040D2857F7FE0112B956D33E7D604o3Z3R) Ф152-ФЗ лицо, осуществляющее обработку ПДн по поручению оператора, не обязано получать согласие субъекта ПДн на обработку его ПДн.

**Типичное нарушение ст. 6 152-ФЗ – «Обработка ПДн без законных оснований»**

Использовать чужие ПДн нельзя просто так. Нужно получить согласие на обработку ПДн, либо убедиться, что закон разрешает вам такую обработку и без согласия гражданина.

**Штраф**: 50тыс.руб. (максимальный штраф для юридического лица). **(ч. 1** [**ст. 13.11**](http://www.consultant.ru/document/cons_doc_LAW_34661/1f421640c6775ff67079ebde06a7d2f6d17b96db/)**КоАП РФ)**

Кроме того, оператор должен заранее определять цели обработки ПДн и соблюдать их. Если вы выходите за пределы заявленных целей, то величина штрафа до 50 тыс. рублей.

**Пример судебной практики.** Суды признали законным предписание Роскомнадзора, выданное в связи с тем, что коммунальная компания без согласия должников передавала сведения о них иной организации – расчетному центру ([Постановление](http://kad.arbitr.ru/PdfDocument/54c24218-e456-49ef-bb50-dce964612563/A71-6910-2013_20140226_Reshenija%20i%20postanovlenija.pdf) ФАС Уральского округа от 26.02.2014 № Ф09-73/14 по делу № А71-6910/2013).

**Типичное нарушение ст. 6 152-ФЗ - «Не обеспечение оператором сохранности/конфиденциальности при хранении материальных носителей ПДн»**

Рассматриваются случаи, когда ПДн обрабатываются без использования вычислительной техники, что не исключает нарушения оператором условий в части безопасности материальных носителей ПДн.

Под безопасностью, в данном случае, подразумеваются условия, при которых носители ПДн, во-первых, остаются в сохранности, а, во-вторых, исключают несанкционированный доступ со стороны третьих лиц.

В связи с этим следует обратить внимание на [Постановление](http://base.garant.ru/193875/) Правительства РФ от 15.09.2008 № 687, утверждающее «Положение об особенностях обработки ПДн, осуществляемой без использования средств автоматизации». Этим документом на операторов возлагаются такие обязанности, как:

* определения мест хранения ПДн и перечня лиц, имеющих к ним доступ;
* раздельное хранение ПДн, обрабатываемых в различных целях;
* самостоятельное определение мер по обеспечению безопасности и сохранности материальных носителей.

Административное наказание применяется в случаях наступления негативных последствий – таких, как неправомерный доступ третьих лиц к ПДн, уничтожение или распространение данных.

**Штраф**: 50 тыс.руб **(ч. 6** [**ст. 13.11**](http://www.consultant.ru/document/cons_doc_LAW_34661/1f421640c6775ff67079ebde06a7d2f6d17b96db/)**КоАП РФ)**

**Пример судебной практики** . Арбитражные суды Московского округа признали законным предписание Роскомнадзора, вынесенное «Почте России». Предписание было выдано в связи с нарушениями, допущенными отделениями в нескольких субъектах РФ, которые заключались в отсутствии мест хранения ПДн и отсутствии перечня лиц, обрабатывающих ПДн / имеющих к ним доступ ([Постановление](http://kad.arbitr.ru/PdfDocument/236b752c-be10-4c78-becf-77d4f1b4cf32/A40-129853-2010_20111011_Reshenija%20i%20postanovlenija.pdf) ФАС Московского округа от 11.10.2011 по делу № А40-129853/10-147-806).

**1.6. Согласие субъекта ПДн на обработку его ПДн (ст. 9 152-ФЗ)**

Согласно [п. 1 ст. 9](consultantplus://offline/ref=DDB676B58918430638255AEFE3F3F95E12E2CB68BC0F1515BBDE878C4FEE068B9622425ED04E05A04E0040D2857F7FE0112B956D33E7D604o3Z3R) 152-ФЗ субъект ПДн принимает решение о предоставлении его ПДН и **дает согласие на их обработку свободно, своей волей и в своем интересе**. Согласие на обработку ПДн должно быть конкретным, информированным и сознательным. Согласие на обработку ПДн может быть дано субъектом ПДн или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено Федеральным законом.

В соответствии с [ч. 2 ст. 9](consultantplus://offline/ref=DDB676B58918430638255AEFE3F3F95E12E2CB68BC0F1515BBDE878C4FEE068B9622425ED04E05AF470040D2857F7FE0112B956D33E7D604o3Z3R) 152-ФЗ согласие на обработку ПДн может быть отозвано субъектом ПДн.

**Типичное нарушение ст.9 152 – ФЗ – «Не получено письменное согласие на обработку ПДн по специальной форме»**

Если письменное согласие не содержит всю информацию согласно перечню из ч. 4 [ст. 9](http://www.consultant.ru/document/Cons_doc_LAW_61801/6c94959bc017ac80140621762d2ac59f6006b08c/) 152-ФЗ, то контролирующими органами будет приравнено к отсутствию согласия.

Письменное согласие по специальной форме требуется, например:

* при обработке особых категорий «ПДн» (речь идет о sensitivedata: сведениях о состоянии здоровья, интимной жизни, национальной принадлежности и т.д.);
* при обработке биометрических данных для установления личности гражданина (в том числе если речь идет об идентификации по фото);
* при передаче ПДн в страну, которая, по мнению Роскомнадзора, не обеспечивает их «адекватную защиту»\* (например, в США, Гонконг или Швейцарию).

\*В последнем пункте речь идет о странах, не являющихся участницами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке ПДн и не перечисленных в [Приказе](http://24.rkn.gov.ru/docs/24/sm19186/PrikazRoskomnadzoraot15.03.2013N274.htm) Роскомнадзора от 15.03.2013 № 274.

**Штраф**: 75 тыс.руб.**(ч. 2** [**ст. 13.11**](http://www.consultant.ru/document/cons_doc_LAW_34661/1f421640c6775ff67079ebde06a7d2f6d17b96db/)**КоАП РФ)**

В определенных случаях нужно получать письменное согласие на обработку ПДн гражданина, которое составляется по определенной форме

**Пример судебной практики.** Компания «Скартел» (бренд Yota) осуществляла трансграничную передачу ПДн в США без получения письменных согласий. Это послужило одним из оснований выдачи Роскомнадзором предписания об устранении нарушений законодательства, которое было признано судами законным ([Постановление](http://kad.arbitr.ru/PdfDocument/5049ab45-d50a-4f2a-ab1a-b652d56e4d6d/A40-17595-2016_20160816_Postanovlenie%20apelljacionnoj%20instancii.pdf) Девятого арбитражного апелляционного суда от 16.08.2016 по делу № А40-17595/16).

**1.7. Право субъекта ПДн на доступ к его ПДн (ст. 14 152-ФЗ)**

Граждане вправе запрашивать информацию, касающиеся обработки их ПДн. Например:

* на каком основании и для чего данные обрабатываются?
* кто имеет доступ к данным, кроме самого оператора и его работников?
* будут ли ПДн передаваться за рубеж?

Если запрос содержит все необходимые реквизиты, подписан субъектом ПДн или его представителем («живой» или электронной подписью), то ответ на него, как правило, обязателен. Оператор вправе отказать в ответе, если в течение последних 30 дней уже дал достаточную информацию по такому же запросу.

**Типичное нарушение ст. 14 152 – ФЗ – «Проигнорирован запрос гражданина о том, как обрабатываются его ПДн»**

**Штраф**: 40 тыс.руб.**(ч. 4** [**ст. 13.11**](http://www.consultant.ru/document/cons_doc_LAW_34661/1f421640c6775ff67079ebde06a7d2f6d17b96db/)**КоАП РФ)**

**Пример судебной практики**. Заемщица обратилась в суд с требованием к микрофинансовой организации «Фреш кэш» предоставить информацию, касающуюся обработки ее ПДн, предоставленных при заключении договора займа. Ответчик не смог представить суду доказательства о направлении ответа на данное требование, поэтому суд не только обязал МФО предоставить запрошенную информацию, но и взыскал символические 2000 ₽ морального вреда (Апелляционное [определение](http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=SARB&n=88473#0) Санкт-Петербургского городского суда от 18.04.2016 № 33-6906/2016 по делу № 2-8320/2015).

**1.9. Обязанности оператора по устранению нарушений законодательства, допущенных при обработке ПДн, по уточнению, блокированию и уничтожению ПДн (ст. 21 152-ФЗ)**

**Типичная ошибка – « не выполнение требования Роскомнадзора об уточнении, блокировании или уничтожении ПДн**

[Ст. 21](http://www.consultant.ru/document/cons_doc_LAW_61801/d3fe43a7c415353b17faab255bc0de92bea127da/) 152- ФЗ устанавливает для операторов специальную процедуру того, что делать, если, по мнению субъекта ПДн или Роскомнадзора, обработка ведется незаконно.

* На период проверки обоснованности запроса ПДн должны быть заблокированы.
* Если ПДн будут окажутся неточными, то их нужно скорректировать в течение 7 рабочих дней после получения уточнений.
* В течение 3 рабочих дней после получения соответствующего запроса неправомерная обработка ПДн должна быть прекращена оператором. Если обеспечить законные основания для обработки не удается в течение 10 рабочих дней, то данные должны быть уничтожены.

Если цели обработки ПДн достигнуты оператором, то использование ПДн нужно прекратить в течение 30 дней, уничтожив ПДн. То же самое касается и случаев, когда согласие субъекта ПДн было им отозвано.

**Штраф**: 45 тыс. руб (**ч. 5** [**ст. 13.11**](http://www.consultant.ru/document/cons_doc_LAW_34661/1f421640c6775ff67079ebde06a7d2f6d17b96db/)**КоАП РФ)**

**Пример судебной практики**. Компания «Скартел» (бренд Yota) не уничтожала ПДн, содержавшиеся в резюме кандидатов, в течение 30 дней после принятия решения о приеме на работу. Это послужило одним из поводов для выдачи предписания Роскомнадзором, которое было признано судами законным ([Постановление](http://kad.arbitr.ru/PdfDocument/5049ab45-d50a-4f2a-ab1a-b652d56e4d6d/A40-17595-2016_20160816_Postanovlenie%20apelljacionnoj%20instancii.pdf) Девятого арбитражного апелляционного суда от 16.08.2016 по делу № А40-17595/16).

**1.10. Реестр операторов ПДн (ст. 23 152-ФЗ)**

Согласно п. 3 ч. 5 ст. 23 152-ФЗ Уполномоченный орган по защите прав субъектов персональных данных обязан вести реестр операторов.

Сведения, содержащиеся в реестре операторов, за исключением сведений о средствах обеспечения безопасности персональных данных при их обработке, являются общедоступными.

Взаимодействие с Роскомнадзором в данной области регулируется:

- **приказом Роскомнадзора от 30.10.2018 № 159** «О внесении изменений в Методические рекомендации по уведомлению уполномоченного органа о начале обработки персональных данных и о внесении изменений в ранее представленные сведения, утверждённые приказом Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 30 мая 2017 года № 94»;

- **приказом Роскомнадзора от 30.05.2017 № 94** "Об утверждении Методических рекомендаций по уведомлению уполномоченного органа о начале обработки персональных данных и о внесении изменений в ранее представленные сведения".

**2. Локализация ПДн в России**

C 1 сентября 2015 года в Российской Федерации начало действовать положение о локализации хранения и отдельных процессов обработки ПДн, определенное в **Федеральном законе от 21 июля 2014 года № 242 – ФЗ** «О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки ПДн в информационно-телекоммуникационных сетях».

Указанным федеральным законом были внесены изменения **Федеральный закон от 27 июля 2006 г. №149 - ФЗ** «Об информации, информационных технологиях и о защите информации», дополнен новой статьёй 15.5 «Порядок ограничения доступа к информации, обрабатываемой с нарушением законодательства Российской Федерации в области ПДн».

В России была создана автоматизированная информационная система «Реестр нарушителей прав субъектов ПДн», целью которой является ограничение доступа к информации в «Интернет», обрабатываемой с нарушением законодательства Российской Федерации в области ПДн. Основанием для внесения в "Реестр нарушителей" доменного имени, URL-адреса интернет-страницы, законодателем установлено вступившее в законную силу решение суда о признании деятельности по распространению информации, содержащей ПДн, нарушающей требования 152 - ФЗ, а также права субъекта ПДн на неприкосновенность частной жизни, личную и семейную тайну.

Деятельность Роскомнадзора по данному направлению регулируется:

-**Федеральным законом от 21 июля 2014 года № 242-ФЗ «**О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях»;

**-постановлением Правительства Российской Федерации от 19 августа 2015 года № 857 «**Об автоматизированной информационной системе "Реестр нарушителей прав субъектов персональных данных";

**- приказом Роскомнадзора от 22 июля 2015 года № 84 «**Об утверждении порядка взаимодействия оператора реестра нарушителей прав субъектов персональных данных с провайдером хостинга и Порядка получения доступа к информации, содержащейся в реестре нарушителей прав субъектов персональных данных, оператором связи»;

**-приказом Роскомнадзора от 28 июля 2015 года № 85 «О**б утверждении формы заявления субъекта персональных данных о принятии мер по ограничению доступа к информации, обрабатываемой с нарушением законодательства Российской Федерации в области персональных данных».

На особом контроле Роскомнадзора находятся рекрутинговые агентства, страховые компании, организации гостиничного и туристического бизнеса, операторы электронной дистанционной торговли, сервисы бронирования билетов в рамках осуществления пассажирских перевозок, кредитные организации, дилерские центры и др

К кампаниям, находящимся в зоне риска можно отнести:

* Зарубежные интернет-сервисы;
* Российские юридические лица, филиалы и представительства иностранных компаний;
* Компании, использующие зарубежные интернет-сервисы (например, сервис для email-рассылок, такой как Mailchimp) для сбора ПДн

Изменения коснулись и содержания уведомления о начале обработке ПДн, которое оператор ПДн обязан подать в Роскомнадзор. С момента вступления в силу 242-ФЗ оператор ПДн должен указывать в уведомлении информацию о месте нахождения базы данных, в которой обрабатываются ПДн российских граждан.

До вступления закона в силу многие операторы ПДн обеспечили перенос баз данных в российские дата-центры.

До 2019 года за нарушение требований о локализации, прописанных в законе РФ No152-ФЗ «О ПДн», могли только заблокировать сайт. Но в конце 2019 года были введены новые штрафы до 18 млн рублей за неисполнение требований о локализации ПДн россиян на территории России.

Основные санкции за нарушение требований:

* Блокировка сайта;
* Приостановка обработки данных;
* Штрафы: до 6 млн руб. за первое нарушение, до 18млн руб. — за повторное.

***Пути минимизации рисков нарушения требований законодательства***

***о локализации ПДН россиян на территории России.***

* Локализация всей системы с БД;
* Локализация БД;
* Отказ от использования ИС;
* Промежуточная БД;
* Отказ от обработки ПДн в ИС;
* Ответственность на подрядчике / Операторе;
* Обезличивание ПДн

**3. Решения, применяемые в SAP, для защиты ПДн**

1. Облачные решения SAP — Ariba (управление процессом закупок) и Success Factors (**система управления кадровыми ресурсами)** размещены в ЦОД (центрах обработки данных, созданных совместно с «Ростелеком»). Это, по заявлению SAP, позволяет российским заказчикам компании хранить свои данные в соответствии с изменившимися требованиями российского закона о персональных данных, в том числе требования от всех компаний, работающих с персональными данными российских граждан, обрабатывать и хранить их на территории РФ. Центр обработки данных SAP в России
2. SAP провела работы по сертификации средств защиты информации, в том числе встроенных в облачные программные продукты SAP, и получила аттестаты соответствия ФСТЭК.
3. Интеграция облака HEC и SAP Сеть DC и корпоративная сеть SAP полностью изолированы. Каждый заказчик получает собственную изолированную инфраструктуру, которая может интегрироваться с корпоративной сетью клиента.
4. Резервное копирование Основной сайт Резервный сайт Каждый час: журнал транзакции Каждый день: инкрементальный Каждая неделя: полный Срок хранения: от 30 дней Ежеквартальное тестирование Резервное копирование: в пределах 24 часов Среднее время восстановления: в пределах 72 часов Процесс резервного копирования подтвержден аудитом.
5. Защита данных на всех этапах в облачных решениях SAP
6. Мониторинг Data Center Регулярное сканирование инфраструктуры Еженедельные тесты на проникновение External Intrusion Detection Perimeter Firewall Internal Intrusion Detection Клиенты Операторы SAP Тесты на проникновение Двухфакторная аутентификация RSA A d m i n V P N Access Contol & Logging (JumpHost) 2016 SAP SE or an SAP affiliate company. All rights reserved. Public 12
7. Соответствие облачных решений SAP требованиям Российского законодательства Сертификация всех функций безопасности, встроенных в ПО, а также наложенных средств защиты информации по требованиям ФСТЭК России Аттестация каждого решения ЦОД по 2-му уровню защищенности ПДн Аттестация HEC по классу 1Г для ИС, обрабатывающих конфиденциальную информацию, включая коммерческую тайну Регистрация САП СНГ в Роскомнадзоре в качестве оператора ПДн Сертификация решений ЦОД по ISO SAP SE or an SAP affiliate company. All rights reserved. Public
8. Аттестаты соответствия информационных систем ЦОДа САП СНГ требованиям безопасности информации Все облачные решения SAP на обеих площадках российского ЦОДа (Ariba, SuccessFactors и HEC) получили Аттестаты соответствия по 2-му уровню защищенности ПДн. Кроме того HEC аттестован по классу 1Г для ИС, обрабатывающих конфиденциальную информацию SAP SE or an SAP affiliate company. All rights reserved. Public 15
9. Лицензии САП СНГ (1): Бессрочная лицензия ФСБ России , рег Н от г. на 12 видов деятельности, включая распространение (продажу), инсталляцию, техническое обслуживание шифровальных (криптографических) средств, предоставление услуг в области шифрования информации. Позволяет: соответствовать требованиям законодательства в вопросах получения по электронным каналам и продажи продуктов SAP, имеющий функции шифрования; предоставлять услуги, включая облачные, на территории РФ по использованию продуктов SAP, имеющий функции шифрования; соответствовать тендерным требованиям заказчиков при создании защищенных информационных систем SAP SE or an SAP affiliate company. All rights reserved. Public 16
10. Лицензии САП СНГ (2): Бессрочные лицензии ФСТЭК России , рег и , рег от г. на деятельность по разработке и производству средств защиты конфиденциальной информации на деятельность по технической защите конфиденциальной информации Позволяют: предоставлять услуги, включая облачные, на территории РФ по использованию продуктов SAP по технической защите конфиденциальной информации, включая персональные данные; соответствовать тендерным требованиям заказчиков при создании защищенных информационных систем SAP SE or an SAP affiliate company. All rights reserved. Public 17
11. Сертификация продуктов SAP
12. Действующие сертификаты на ПО SAP Федеральная Служба по Техническому и Экспортному Контролю РФ (ФСТЭК России) SAP NetWeaver 7.02 сертификат 2395 (ABAP) от , 2873 (Java) от Позволяет использовать SAP NW для построения систем, обрабатывающих конфиденциальную информацию Позволяет использовать SAP NW для построения типовых информационных систем персональных данных (ИСПДн) самого высокого уровня К1 Министерство Обороны Российской Федерации (МО РФ)\* SAP NetWeaver 2004 сертификат 779 от Позволяет использовать SAP NW для построения систем, обрабатывающих информацию, составляющую государственную тайну не выше уровня «секретно» SAP NetWeaver 7.02 и SAP ERP 6.05 заключения 8 Управления ГШ МО РФ от Позволяет использовать SAP NW и SAP ERP для построения систем, обрабатывающих информацию, составляющую государственную тайну не выше уровня «секретно»\*\* \* Сертификаты и Заключения ГШ МО РФ являются документами с грифом ДСП. Копии могут быть предоставлены конечному заказчику при наличии у него соответствующих допусков. \*\* Возможно повышение уровня секретности обрабатываемой информации при соблюдении дополнительных условий указанных в Заключении 2016 SAP SE or an SAP affiliate company. All rights reserved. Public 19
13. Действующие сертификаты на ПО ЦОД SAP Федеральная Служба по Техническому и Экспортному Контролю РФ (ФСТЭК России) Облачные решения SAP прошедшие сертификацию: HANA Enterprise Cloud Success Factors Ariba Полученные сертификаты ФСТЭК России позволили успешно провести аттестацию облачных информационных систем ЦОД SAP по 2-му уровню защищенности для ИС ПДн SAP SE or an SAP affiliate company. All rights reserved. Public 20
14. Запланированные сертификационные испытания Федеральная Служба по Техническому и Экспортному Контролю РФ (ФСТЭК России) SAP Afaria 7 проводится экспертиза сертификационных испытаний: Позволяет использовать SAP Afaria в составе информационных систем, обрабатывающих конфиденциальную информацию SAP HANA 1.0 завершена экспертиза сертификационных испытаний: Позволяет использовать SAP HANA в составе информационных систем, обрабатывающих конфиденциальную информацию SAP NetWeaver 7.5 начата подготовка к проведению сертификационных испытаний: Позволяет использовать SAP Netweaver и решения на его базе для построения информационных систем, обрабатывающих конфиденциальную информацию 2016 SAP SE or an SAP affiliate company. All rights reserved. Public 21

Вышеуказанные и некоторые другие технические решения и внедренные средства защиты данных делают SAP «привлекательной» для применения в кампаниях, особенно с большой численностью работников, в том числе для защиты их ПДн, а также при необходимости обработки больших массивов данных, и соблюдению требований российского законодательства при взаимодействии с иностранными партнерами.

**4. Трансграничная передача ПДн**

*В соответствии со ст. 12 152-ФЗ:*

*1. Трансграничная передача персональных данных на территории иностранных государств, являющихся сторонами* [*Конвенции*](consultantplus://offline/ref=437ADE859CCB2594FD55A9D94DCB5857CD9370D4934E1E10AC9E4D61C7F9753F81C1FB19C2C3252570C3791E9BPCc2R) *Совета Европы о защите физических лиц при автоматизированной обработке персональных данных, а также иных иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных, осуществляется в соответствии с настоящим Федеральным законом и может быть запрещена или ограничена в целях защиты основ конституционного строя Российской Федерации, нравственности, здоровья, прав и законных интересов граждан, обеспечения обороны страны и безопасности государства.*

*2. Уполномоченный орган по защите прав субъектов персональных данных утверждает* [*перечень*](consultantplus://offline/ref=437ADE859CCB2594FD55A9D94DCB5857CF9076D599441E10AC9E4D61C7F9753F93C1A315C0C63B247AD62F4FDD97E63B320EDADD10CE4321P6c8R) *иностранных государств, не являющихся сторонами* [*Конвенции*](consultantplus://offline/ref=437ADE859CCB2594FD55A9D94DCB5857CD9370D4934E1E10AC9E4D61C7F9753F81C1FB19C2C3252570C3791E9BPCc2R) *Совета Европы о защите физических лиц при автоматизированной обработке персональных данных и обеспечивающих адекватную защиту прав субъектов персональных данных. Государство, не являющееся стороной* [*Конвенции*](consultantplus://offline/ref=437ADE859CCB2594FD55A9D94DCB5857CD9370D4934E1E10AC9E4D61C7F9753F81C1FB19C2C3252570C3791E9BPCc2R) *Совета Европы о защите физических лиц при автоматизированной обработке персональных данных, может быть включено в перечень иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных, при условии соответствия положениям указанной* [*Конвенции*](consultantplus://offline/ref=437ADE859CCB2594FD55A9D94DCB5857CD9370D4934E1E10AC9E4D61C7F9753F81C1FB19C2C3252570C3791E9BPCc2R) *действующих в соответствующем государстве норм права и применяемых мер безопасности персональных данных.*

*3. Оператор обязан убедиться в том, что иностранным государством, на территорию которого осуществляется передача персональных данных, обеспечивается адекватная защита прав субъектов персональных данных, до начала осуществления трансграничной передачи персональных данных.*

*4. Трансграничная передача персональных данных на территории иностранных государств, не обеспечивающих адекватной защиты прав субъектов персональных данных, может осуществляться в случаях:*

*1) наличия согласия в письменной форме субъекта персональных данных на трансграничную передачу его персональных данных;*

*2) предусмотренных международными договорами Российской Федерации;*

*3) предусмотренных федеральными законами, если это необходимо в целях защиты основ конституционного строя Российской Федерации, обеспечения обороны страны и безопасности государства, а также обеспечения безопасности устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства;*

*4) исполнения договора, стороной которого является субъект персональных данных;*

*5) защиты жизни, здоровья, иных жизненно важных интересов субъекта персональных данных или других лиц при невозможности получения согласия в письменной форме субъекта персональных данных.*

По условию кейса резюме кандидатов на вакантные должности топ-уровня необходимо переслать в головной офис кампании в Голландию.

Голландия входит в Перечень из 47 государств, обеспечивающих адекватную защиту персональных данных и являющихся сторонами **108 Конвенцию Совета Европы защите физических лиц при автоматизированной обработке персональных данных и обеспечивающих адекватную защиту прав субъектов персональных данных (Страсбург, 28 января 1981 г.)**

Все страны, которые подписали **Страсбургскую Конвенцию** считаются способными обеспечивать достаточную защиту прав и интересов субъекта. Также существует официальный список, принятый Роскомнадзором, стран, которые тоже удовлетворяют требованиям защиты информации при переводе через границу.

Согласно 152-ФЗ передача сведений через границу может быть запрещена по причине: защиты конституционного строя Российской федерации; нравственности; здоровья; прав и законных интересов граждан РФ; национальной безопасности.

В то же время, трансграничная передача персональных данных в страны, которые не способны обеспечить достаточную защиту такой информации, разрешена только в нескольких случаях: *было получено письменного согласие соответствующего субъекта на трансграничную передачу персональных данных; трансграничная передача данных разрешена по условиям международным договоров, участником которых является Россия; перевод информации в другую страну разрешен по условиям принятых законов, если это необходимо для защиты конституционного строя РФ, государственной безопасности, а также поддержания жизнеспособности транспортной системы, защиты интересов лиц, общества, государства в транспортной сфере при незаконном вторжении; отправка конфиденциальных сведений осуществляется для выполнения контракта, участником которого является субъект; передача данных через границу требуется для защиты жизни субъекта, его здоровья или иных важных интересов, а получение письменного согласие лица не является возможным.*

**Пошаговая инструкция организации трансграничной передачи ПДн.**

Для того, чтобы осуществить перевод конфиденциальных сведений в другую страну необходимо:

* 1. Удостовериться в Роскомнадзоре, является ли страна, в которую планируется перевод, участником Страсбургской Конвенции или же находится в приказе Роскомнадзора “Об утверждении Перечня иностранных государств, не являющихся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных и обеспечивающих адекватную защиту прав субъектов персональных данных”.
  2. Получить согласие соответствующего субъекта ПДн на их обработку для выполнения трансграничной передачи.
  3. Подписать договор со стороной, которая становится получателем данных.
  4. Проверить каналы передачи информации. Для надежной отправки данных необходимо провести защиту каналов передачи персональной информации. Если же эта операция производится через Интернет или через другие незащищённые каналы, то рекомендуется использовать средства шифрования.
  5. Обычно не требуется регистрация в Роскомнадзоре или одобрение письменного согласия для трансграничной передачи. Согласие должно быть просто подписано соответствующим субъектом. Однако необходимо уведомить Роскомнадзор о трансграничной передаче ПДн.
  6. **Ответственность за незаконные действия:**
  + Если же об использовании конфиденциальных сведений не будет сообщено в Роскомнадзор, то это будет считаться незаконным переводом информации в другую страну. Это является нарушением статьи 19.7 Административного Законодательства РФ – штраф 5 тыс.руб.
  + Если уведомление Роскомнадзора будут совершено после того, как ПДн будут обработаны, то это будет таким же правонарушением. Оформление согласия Правила заполнения этого документа описаны в 152- ФЗ. Его содержание является достаточно произвольным, однако нужно помнить о необходимых элементах заявления: Фамилия, имя, отчество субъекта, его адрес и серия, номер паспорта или иного документа, удостоверяющее личность гражданина. Фамилия, имя, отчество лица или название организации, которое, предполагается, будет выполнять обработку. Цели, для которых выполняется выяснение персональных данных. Список сведений, которые будут обработаны. Информация об организации, которая будет совершать дальнейшие операции с данными. Описание того, какие действия будут происходить с данными. Срок, в течение которого действует согласие субъекта. Подпись лица, выполненная лично. Также в ч. 1 ст.9 152- ФЗ описаны критерии, которым должен соответствовать документ о согласии. Главными же из них являются добровольное заполнение заявление и присутствие необходимых элементов в нём. Заявление необходимо предоставить строго в письменной форме, но возможно это сделать и через Интернет. Общепринятой же формы заполнения не существует.

Осуществление передачи персональных данных трансграничным способом и перевод подобных данных в другую страну является ещё более сложным явлением, так как зачастую необходимо учитывать законы несколько государств и международных организаций, в том числе **европейский «Регламент защиты персональных данных» (General** **Data** **Protection** **Regulation, GDPR** .

**5. Особенности получения и обработки ПДн кандидатов на вакантные должности на территории России.**

**в SAP, для защиты ПДн**

**Категории граждан, персональные данные**

**которых, обрабатываются Работодателем**

Кандидаты на вакантные должности

Родственники

работников

работники

Лица, с которыми заключены ГПД

Бывшие работники

Прикомандированные работники

При организации работы с ПДн кандидатов на вакантные должности необходимо изучить Разъяснения Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 14 декабря 2012 г. "Вопросы, касающиеся обработки персональных данных работников, соискателей на замещение вакантных должностей, а также лиц, находящихся в кадровом резерве".

При проведении проверок представители Роскомнадзора считают неправомерным деление лиц, чьи ПДн обрабатываются в кампании на работников кампании и лиц, с которыми нет трудовых отношений.

В соответствии с требованиями законодательства в области обработки ПДн целесообразно определить категории лиц в зависимости **от целей обработки ПДн, объема обработки ПДн и сроков хранения ПДН с учетом деятельности кампании.**

**Источники поступления ПДн кандидатов на вакантные должности**

1

от представителя кадрового агентства

4

Заполнение анкеты непосредственно в службе управления персоналом

3

Направление резюме кандидатом на эл.почту работодателя

2

Резюме, размещенные кандидатом в Интернете на сайтах объявлений

Кандидат на вакантную должность обращаясь в кадровое агентство либо размещая своё резюме на специализированных сайтах по поиску работы, заполняет согласие на обработку ПДн и передачу их третьим лицам в целях рассмотрения его кандидатуры на вакантную должность.

При обращении непосредственно в службу управления персонала, до заполнения каких-либо документов, содержащих ПДн, кандидату будет предложено дать согласие на обработку его ПДн и передачу третьим лицам с указанием цели обработки и передачи ПДН, а также сроков из хранения.

В случае, если сбор персональных данных соискателей осуществляется посредством типовой формы анкеты соискателя, утвержденной оператором, то данная типовая форма анкеты должна соответствовать требованиям п. 7 Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденного постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687, а также содержать информацию о сроке ее рассмотрения и принятия решения о приеме либо отказе в приеме на работу.

Типовая форма анкеты соискателя также может быть реализована в электронной форме на сайте организации, где согласие на обработку персональных данных подтверждается соискателем путем проставлением отметки в соответствующем поле, за исключением случаев, когда работодателем запрашиваются сведения, предполагающие получение согласия в письменной форме.

Если резюме кандидат направил на электронную почту работодателя, то прежде, чем приступить к обработке резюме, необходимо удостовериться в подлинности документа, запросив электронный образ согласия кандидата на обработку его ПДн и передачу третьим лицам с указанием цели обработки и передачи ПДН, а также сроков из хранения. С предоставлением в последующем оригинала согласия в службу управления персоналом. Данный способ получения согласия должен быть прописан в ЛНА.

При рассмотрении документов иностранного гражданина, претендующего на вакантную должность Работодателю необходимо, помимо документов предоставляемым при приеме на работу в соответствии с Трудовым кодексом РФ, удостовериться в наличии у кандидата действующих документов, подтверждающих законность пребывания на территории России, наличие патента (при необходимости), полиса ДМС, прививок от кори, тест на новую коронавирусную инфекцию и иные документы, в соответствии с действующим миграционным законодательством.

Поскольку по условиям кейса на согласование глобальному HR необходимо отправлять документы только на кандидатов, претендующих на «топовые» вакантные должности, то они должны предоставить письменное согласие на трансграничную передачу их ПДн. Учитывая, что существует вероятность, удаленного рассмотрения резюме кандидатов, предлагается предусмотреть в ЛНА возможность получения электронного образа согласия кандидата на трансграничную передачу ПДн

Отдельно необходимо обратить внимание на *обработку персональных данных близких родственников кандидата на вакантную должность* или работника в объеме, предусмотренном унифицированной формой № Т-2, утвержденной постановлением Госкомстата Российской Федерации от 05.01.2004 № 1 «Об утверждении унифицированных форм первичной учетной документации по учету труда и его оплаты», либо в случаях, установленных законодательством Российской Федерации (получение алиментов, оформление допуска к государственной тайне, оформление социальных выплат).

В иных случаях, получение согласия близких родственников работника является обязательным условием обработки их персональных данных.

В случае отказа в приеме на работу сведения, предоставленные соискателем, должны быть уничтожены в течение 30 дней, за исключением случаев, предусмотренных законодательством о государственной гражданской службе, где срок хранения персональных данных соискателя определен в течение 3 лет.

Обработка ПДн работников, включенных в кадровый резерв, и являющихся кандидатами на вакантные должности.

Ведение кадрового резерва на сегодняшний день трудовым законодательством не регламентировано. В этом случае, обработка персональных данных лиц, включенных в кадровый резерв, может осуществляться только с их согласия, за исключением случаев нахождения в кадровом резерве действующих сотрудников, в трудовом договоре которых определены соответствующие положения.

Согласие на внесение соискателя в кадровый резерв организации оформляется либо в форме отдельного документа либо путем проставления соискателем отметки в соответствующем поле электронной формы анкеты соискателя, реализованной на сайте организации в сети Интернет.

Обязательным является условие ознакомления соискателя с условиями ведения кадрового резерва в организации, сроком хранения его персональных данных, а также порядком исключения его из кадрового резерва.

Для кандидатов на вакантные должности государственной гражданской службы несколько иной порядок работы с ПДн, однако по условиям кейса, трудоустройство госслужащих в кампанию вряд ли возможно.

**6. Организация работы по обработке ПДн работников и**

**кандидатов на вакантную должность**

**в SAP, для защиты ПДн**

1. Провести внутренний аудит для определения чьи и какие персональные данные вы используете, с какой целью и в каком объеме
2. Издать локальные нормативные акты, в которых закрепить порядок обработки ПДн субъектов, их права и обязанности в этой области, в том числе:

* Политика ПДн,
* Положение о ПДН, включая механизм удаления(уничтожения) ПДн.
* Положение о конфиденциальности,

1. Ознакомить работников кампании под роспись с ЛНА о защите ПДн
2. Получить письменное согласие/несогласие на обработку ПДн работников кампании.
3. Определить должностное лицо, ответственное за работу с ПДн
4. Установить перечень лиц с доступом к ПДн с обязательным оформлением ими обязательств о неразглашении ПДн.
5. Определить место хранения ПДн.
6. Провести лицензированный аудит рабочих мест, где обрабатываются ПДн, и технических средств передачи ПДн с целью установления соответствия степени защиты ПДн нормативным требованиям Роскомнадзора и ФСБ России.
7. В Роскомнадзор для включения в Реестр операторов, сдается уведомление установленной формы и документы, по результатам аудита.
8. Получить до трансграничной передачи ПДн письменное согласие работников либо кандидатов на вакантные должности о согласии на трансграничную передачу их ПДн с указанием цели передачи и срока использования.
9. Сервер, на котором находятся ПДн, должен находиться на территории России. За границу передается копия базы данных, содержащей ПДн приусловии выполнения п.10.
10. Уничтожать ПДн после того, как достигнете целей их обработки с составлением акта уничтожения.