**ИПК «ИГРА В КАРЫ»**

**Вводные данные:**

Численность компании**:** 8000 человек

Количество открытых вакансий в месяц: 250

Количество соискателей в месяц: 1500-2000 человек

Соискатели: граждане РФ, иностранные граждане

Головная компания: Нидерланды

Используемая HRP система: SAP

**Постановщик задачи**: директор по персоналу

**Исполнитель задачи**: руководитель службы управления персоналом

**Задача:** построить программу работы с персональными данными кандидатов, которых мы рассматриваем на вакантные должности в компании.

Поскольку процесс отбора кандидатов у нас состоит из нескольких этапов, рассматривать мы его будем также поэтапно.

**Этап первый – получение резюме.**

Получать резюме мы можем из нескольких источников (особенно учитывая, что количество резюме у нас колоссальное).

1. Мы размещаем вакансии на сайте компании, где кандидаты могут: **а)** заполнить стандартную форму резюме или **б)** приложить свое резюме в любом формате;
2. У нас есть адрес электронной почты (например, указанный на нашем сайте), куда кандидаты могут присылать свои резюме;
3. Нам присылают резюме агентства по подбору персонала;
4. Мы получаем резюме с сайтов о работе (путем отклика кандидатов или прямого поиска резюме рекрутером);
5. У нас есть программа «Приведи друга», через которую наши собственные работники рекомендуют нам кандидатов и приносят их резюме в отдел подбора персонала;
6. У нас есть ресепшн или проходная (или, например, офисы или точки продаж), где есть бланки анкет, которые может заполнить любой желающий и опустить в специальный ящик или передать сотруднику;
7. Прямой поиск через социальные сети и профильные сообщества, хантинг.

Резюме – это документ, который заведомо содержит целый ряд персональных данных, и в том числе может содержать биометрические данные:

* паспортные данные;
* место проживания;
* личный телефон и адрес электронной почты (или мессенджеров);
* семейное положение и наличие детей;
* сведения об образовании, профессиональные навыки;
* опыт работы;
* фотография и видео (для некоторых, особенно творческих профессий, распространена такая форма, как видеорезюме) - биометрические персональные данные.

Поскольку мы еще не вступили с кандидатом в трудовые отношения, а значит, не можем ссылаться на п.5 ч.1 ст.6 Федерального закона «О персональных данных» (здесь и далее № 152-ФЗ) который разрешает нам не брать согласие на обработку персональных данных, если она *«необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных*», то нам необходимо получить согласие субъекта персональных данных на их обработку в соответствии с п.1 ч.1 ст.6 № 152-ФЗ.

Казалось бы, для обработки биометрических персональных данных мы к тому же обязаны взять согласие кандидата только в письменной форме (ч.1 ст. 11 и ч.4 ст. 9 № 152-ФЗ), но внимательно изучив положения ч.1 ст. 11 мы видим, что это *«сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность (биометрические персональные данные) и которые используются оператором для установления личности субъекта персональных данных…».* Т.е. таким сведениям не обязательно просто характеризовать физиологические и биологические особенности человека, они еще должны **давать возможность** установить его личность, и они должны **использоваться** оператором именно для установления личности. В случае с резюме у нас есть данные, которые и без фото и видео вполне устанавливают личность кандидата, и, соответственно, его биометрические данные не используются нами для таковых целей.

**Рассмотрим наш порядок действий при получении резюме из разных источников:**

1. Определим, что для любого вида работы с веб-сайтом компании нам будет необходимо обеспечить неограниченный доступ через Интернет к документу, который определяет Политику организации в отношении обработки персональных данных, включая соблюдение требований о конфиденциальности (ч. 2 ст. 18.1 № 152-ФЗ, рекомендации Роскомнадзора от 27.07.2017). Кроме политики нужно разместить на сайте сведения о том, какие меры принимает владелец сайта, чтобы защитить персональные данные. Можно разместить оба этих документа на одной странице. Также можно сделать ссылки на эту страницу при получении согласия от кандидата.
   1. Согласие субъекта в рамках ч.1 ст.9 № 152-ФЗ должно быть:

* конкретным – а это значит, что мы должны максимально описать перечень персональных данных, которые мы будем обрабатывать или определить, что перечень обрабатываемых персональных данных находится в рамках целей его обработки (такая позиция тоже принимается Роскомнадзором);
* информированным – т.е. мы должны четко прописать цели такой обработки (замещение вакантной должности и внесение в кадровый резерв);
* осознанным – т.е. субъект сделал это самостоятельно, своей волей и в своем интересе.
  1. Также, в соответствии с ч.2 ст.9 № 152-ФЗ мы должны проинформировать субъекта ПДн, что у него есть право на отзыв согласия и предоставить ему возможность этим правом воспользоваться. Соответственно я рекомендую завести отдельный адрес электронной почты, на который кандидаты могут прислать отзыв своего согласия, который также указан на сайте компании в Политике организации в отношении обработки персональных данных, чтобы такие запросы не потерялись в обще почте (мы должны прекратить обработку в случае отзыва и уничтожить их в течение 30 дней с даты поступления указанного отзыва, ч.5 ст.21 № 152-ФЗ).
  2. А также мы должны указать право субъекта персональных данных на доступ к ним в соответствии со ст.14 № 152-ФЗ, для чего также рекомендуется указать способы направления таких обращений.

**См. Рекомендации Роскомнадзора от 27.07.2017 по составлению документа, определяющего политику оператора в отношении обработки персональных данных, в порядке, установленном федеральным законом от 27 июля 2006 года № 152-ФЗ "О персональных данных"**

|  |  |  |  |
| --- | --- | --- | --- |
| **Источник получения резюме** | **Способ получения согласия на обработку ПДн** | **Нормативный документ** | **Действия компании** |
| **Сайт компании** | "Типовая форма анкеты соискателя может быть реализована в электронной форме на сайте организации, где согласие на обработку персональных данных подтверждается соискателем путем проставления отметки в соответствующем поле, за исключением случаев, когда работодателем запрашиваются сведения, предполагающие получение согласия в письменной форме." "Обработка персональных данных соискателей на замещение вакантных должностей в рамках правоотношений, урегулированных Трудовым кодексом РФ, предполагает получение согласия соискателей на замещение вакантных должностей на обработку их персональных данных на период принятия работодателем решения о приеме либо отказе в приеме на работу." "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." | Разъяснения Роскомнадзора от 14.12.2012 "Вопросы, касающиеся обработки персональных данных работников, соискателей на замещение вакантных должностей, а также лиц, находящихся в кадровом резерве." | Поскольку контроллер допускает сбор согласий через сайт, в случае проверки, мы должны будем показать, как у нас устроен автоматизированный сбор согласий.  Для этого в ЛНА нужно прописать, что такой порядок установлен, что предоставление данных без проставления отметки в соответствующем поле невозможно, система просто этого не допустит. Можно в ЛНА приложить скрин-шоты процесса направления резюме.  Также в этом ЛНА должен быть утвержден текст согласия на обработку персональных данных, которое мы публикуем на сайте. В согласии должно быть прописано, что обработка персональных данных будет производиться с целью рассмотрения на замещение вакантной должности и в период принятия работодателем решения о приеме на работу.  Целесообразнее все же разработать свою форму резюме для заполнения, чтобы четко определить перечень ПДн, и чтобы соискатель случайно не направил специальную категорию персональных данных, для обработки которой нам необходимо письменное согласие. |
| **Кадровые агентства** | Тут есть два варианта:  1. Мы заключаем договор с кадровым агентством (КА), по которому они являются обработчиком ПДн и сами собирают и передают нам для конкретных целей (замещение вакантной должности и создание кадрового резерва) персональные данные как субобработчику. В этом случае они несут полную ответственность за заключение согласия с кандидатом. Мы же обеспечиваем защиту и конфиденциальность ПДн в рамках договора.  2. Мы заключаем договор с КА, по которому мы являемся оператором и обработчиком, а они субобработчиком, но мы наделяем их ответственностью за сбор согласий от кандидатов на обработку персональных данных нами (по принципу покупки сим-карты в салоне сотовой связи, где согласие берет сам салон, а оператором является оператор сотовой связи). | ч.3-5 ст. 6 № 152-ФЗ, Рекомендации Роскомнадзора от 27.07.2017 по составлению документа, определяющего политику оператора в отношении обработки персональных данных, в порядке, установленном федеральным законом от 27 июля 2006 года № 152-ФЗ "О персональных данных"  "В случае необходимости взаимодействия с третьими лицами в рамках достижения целей обработки персональных данных рекомендуется указывать условия передачи персональных данных в адрес третьих лиц (например, наличие договора поручения на обработку персональных данных), в том числе, находящихся за пределами Российской Федерации (трансграничная передача). При этом рекомендуется указать конкретное наименование и местонахождение соответствующих третьих лиц, цели осуществляемой (трансграничной) передачи, объем передаваемых персональных данных, перечень действий по их обработке, способы и иные условия обработки, включая требования к защите обрабатываемых персональных данных." | Необходимо определиться с типом заключения договора с КА (я думаю, предпочтительнее вариант 1), этого будет достаточно для реализации этого способа получения резюме.  При варианте 2 мы должны получать вместе с резюме подписанный кандидатом согласия. |
| **Резюме с сайтов о работе** | Самый простой вариант - все взаимодействия с кандитом регулирует сам сайт о работе, который получает согласие в рамках своей оферты на размещение соискателем своего резюме в сети Интернет, доступного неограниченному кругу лиц. | Разъяснения Роскомнадзора от 14.12.2012 "Вопросы, касающиеся обработки персональных данных работников, соискателей на замещение вакантных должностей, а также лиц, находящихся в кадровом резерве." | Есть принципиальное ограничение - взаимодействие до приглашения кандидата на интервью со всем кандидатами, откликнувшимся на вакансию или просто разместившими свое резюме на сайте о работе должно проходить только и исключительно в рамках этого сайта. В рамках своей оферты владелец сайта выступает в качестве оператора и несет ответственность перед субъектом. Как только мы сохраняем или распечатываем любое резюме с сайта о работе, мы автоматически должны получить согласие кандидата, поскольку теперь наши отношения регулируются напрямую, и мы теперь являемся оператором ПДн. Поэтому, рекомендую использовать возможности сайтов по работе с резюме (включая приглашения на собеседование). Но, если это невозможно, то высылать интересным кандидатам письма с просьбой дать согласие на обработку ПДн, поскольку обязанность предоставить доказательство на получения согласия лежит теперь на нас. |
| **Резюме на определенный электронный адрес компании** | Если работодатель получает резюме соискателя по электронной почте, ему нужно дополнительно провести мероприятия, которые бы служили подтверждением факта направления резюме самим соискателем, согласие также нужно получить любым способом, т.к. этот случай не является исключением даже несмотря на то, что кандидат сам с нами связался.  Исключениями являются только два случая:  - от имени соискателя действует кадровое агентство, с которым у него договор;  - соискатель сам разместил резюме в сети Интернет, доступное неограниченному кругу лиц. | Разъяснения Роскомнадзора от 14.12.2012 "Вопросы, касающиеся обработки персональных данных работников, соискателей на замещение вакантных должностей, а также лиц, находящихся в кадровом резерве."  "В случае получения резюме соискателя по каналам электронной почты, факсимильной связи работодателю необходимо дополнительно провести мероприятия, направленные на подтверждение факта направления указанного резюме самим соискателем. К примеру, к таким мероприятиям можно отнести приглашение соискателя на личную встречу с уполномоченными сотрудниками работодателя, обратная связь посредством электронной почты и т.д." "При поступлении в адрес работодателя резюме, составленного в произвольной форме, при которой однозначно определить физическое лицо, его направившее, не представляется возможным, данное резюме подлежит уничтожению в день поступления." | Если у нас не настроен сбор согласий через сайт компании (где как раз и указан адрес, на который нужно отправлять резюме), то крайне желательно настроить хотя бы автоматическую рассылку с этого адреса электронной почты ответов на входящие письма с просьбой направить в адрес компании ответ с согласием на обработку ПДн. В противном случае рассылку придется делать рекрутеру. Согласие может быть выражено как в теле ответного письма (лучше сразу указать в письме, какой фразой кандидату оптимально давать такое согласие), либо фото распечатанного и подписанного согласия (что не всегда возможно для кандидата). |
| **Рекомендации работников** | Когда мы анонсируем такую программу, мы должны уведомить своих работников, что мы сможем принимать резюме от их знакомых только через сайт, на выделенный адрес электронной почты, либо они могут принести нам его в бумажном виде. Во втором случае они должны одновременно с резюме принести согласие на обработку ПДн, подписанное кандидатом. Такое согласие работники и кандидаты могут скачать на сайте компании или обратиться в отдел персонала.  В случае, если работник все же принесет только резюме, то придется связаться с кандидатом, чтобы убедиться, что резюме прислал сам соискатель, либо уничтожить его. "При поступлении в адрес работодателя резюме, составленного в произвольной форме, при которой однозначно определить физическое лицо, его направившее, не представляется возможным, данное резюме подлежит уничтожению в день поступления." | Разъяснения Роскомнадзора от 14.12.2012 "Вопросы, касающиеся обработки персональных данных работников, соискателей на замещение вакантных должностей, а также лиц, находящихся в кадровом резерве." Постановлением Правительства РФ от 15.09.2008 №687 "Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации" | Требуется разработать и разместить в доступе вариант согласия на обработку ПДн кандидатов в версии для печати.  Поскольку мы будем обрабатывать ряд резюме на бумажных носителях, мы должны либо руководствоваться Постановлением Правительства РФ от 15.09.2008 №687, либо перевести данную информацию информационную систему (что предпочтительно). |
| **Получение заполненной анкеты в бумажном виде** | В этом случае у нас есть бумажный носитель, который сразу может содержать в себе форму согласия на обработку резюме для целей рассмотрения кандидата на вакантную должность и занесения сведений анкеты в информационную систему для создания кадрового резерва. | п. 7 "Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации." (утверждено Постановлением Правительства РФ от 15.09.2008 N 687) | При обработке материальных носителей персональных данных мы автоматически попадаем под действие указанного сдесь положения, поэтому должны разработать анкету с соблюдением его требований: -анкета должна содержать информацию о сроке её рассмотрения и принятия решения о приеме либо отказе в приеме на работу; -в анкете должны быть сведения о цели обработки персональных данных, имя (наименование) и адрес оператора, ФИО и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых работодателем способов обработки данных; -в анкете должно быть поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку; -анкета должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими данными, не нарушая прав и законных интересов других; -в анкете не должно быть предусмотрено объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы; - в анкете должен быть указан способ связи с оператором, по которому кандидат может реализовать свое право на доступ к своим ПДн и направить отзыв своего согласия. |

В случаях прямого поиска специалистов, а также хантинга менеджеров высшего звена мы с большой долей вероятности будем просить человека либо предварительно выслать нам свое резюме, поэтому направим ему согласие на обработку по почте, либо сразу пригласим его на встречу, где подпишем бумажное согласие.

1. Во-вторых, если мы хотим (а мы хотим ☺) в получить также согласие кандидата на последующее включение его данных в кадровый резерв для рассмотрения его кандидатуры на аналогичные или другие вакансии, возникающие в компании, нам необходимо взять такое согласие отдельно. Это может быть один документ, с двумя отметками о согласии на обработку ПДн в целях рассмотрения на замещение вакантной должности и для включения в кадровый резерв.

*«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.»*

*Разъяснения Роскомнадзора от 14.12.2012 "Вопросы, касающиеся обработки персональных* данных работников, соискателей на замещение вакантных должностей, а также лиц, находящихся в кадровом резерве."

1. Что обязательно нужно указать в согласии:

* наименование и адрес оператора;
* цели обработки персональных данных (они обязательно должны быть привязаны к реальному процессу компании, например, ведение кадрового резерва);
* перечень персональных данных, на обработку которых дается согласие (не допускаются формулировки типа «и иные данные», если нет возможности точно определить перечень данных, то опять же привязываемся в процессу, например, «данные, указанные кандидатом в резюме»);
* перечень действий с персональными данными (все, кроме распространения – этого мы не делаем!);
* срок действия согласия субъекта (и/или условия прекращения обработки, например, достижение целей обработки) и порядок его отзыва.

Согласие может быть получено любым путем, позволяющим подтвердить его получение и не должно нарушать права субъекта ПДн.

1. При рассмотрении кандидатов на вакантные должности **нельзя!** использовать данные из социальных сетей. Т.к. понятие общедоступная информация и общедоступные источники персональных данных – это не одно и то же. При размещении ПДн в общедоступных источниках требуется письменное согласие субъекта. Если Роскомнадзор при проверке найдет у нас такие сохраненные данные, то это будет нарушением.

До сих пор продолжается судебное разбирательство между ООО «В КОНТАКТЕ», ООО «ДАБЛ» (российское подразделение, использующее технологию скорринга Double Data) и АО «Национальное бюро кредитных историй» (НБКИ). Несмотря на то, что дело еще не завершено, Роскомнадзор озвучил позицию, что такие данные собирать нельзя.

1. Информационные системы безопасности, в которых ведется база кандидатов и кадровый резерв должны соответствовать требованиям, установленным Постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
2. Поскольку у нас есть иностранные кандидаты, но иное обращение с их персональными данными не предусмотрено № 152-ФЗ, то согласно ст. 2.1 ГК РФ правила, установленные гражданским законодательством, применяются к отношениям с участием иностранных граждан, лиц без гражданства и иностранных юридических лиц, если иное не предусмотрено федеральным законом. Нюансы возникнут при транграничной передаче ПДн таких кандидатов, но на этапе получения согласия они равны с гражданами РФ.
3. Кандидаты должны быть проинформированы о том, что они могут отказаться дать свое согласие, но в этом случае мы не сможем рассматривать их на вакантную позицию, т.к. не будем иметь для этого права.

**Этап второй – передача резюме нанимающему руководителю, проведение им собеседований.**

1. Поскольку руководители имеют доступ к ПДн, то они должны быть перечислены в утвержденном перечне должностей, имеющих такой доступ, с ними должны быть заключены соглашения о доступе к определенным категориям ПДн и обязательства о неразглашении такой информации.
2. Оптимальным обеспечением защиты персональных данных, минимизации рисков утечки ПДн и разграничения прав доступа к ним будет ведение базы данных кандидатов в электронном виде, где каждый руководитель будет получать доступ только к «своим» кандидатам и сможет работать с резюме без бумажных носителей.
3. Также я рекомендую проводить в компании внутреннее обучение по порядку работы с ПДн для лиц, у которых есть доступ, поскольку нарушения в этой сфере очень часты. Например, руководитель может направить интересные резюме, которые остались после закрытия позиции, своему коллеге в другой компании, чтобы порекомендовать ему людей, которых он уже собеседовал. Это делать без согласия кандидата запрещено!
4. Поскольку мы направляем резюме руководителю, это значит, что мы уже вышли за контуры работного сайта, и мы обязаны к этому моменту получить согласие на обработку персональных данных с любого из таких кандидатов.
5. При приглашении кандидата на личную встречу с руководителем в офисе компании мы должны обеспечить неограниченный доступ к нашей Политике организации в отношении обработки персональных данных (например, кандидат мог не видеть ее на сайте, потому что он туда никогда не заходил), поэтому бумажный вариант Политики можно повесить или разместить в переговорных комнатах, где будут проводиться собеседования.
6. Необходимо подписать с кандидатом согласие на обработку его ПДн, в том числе тех, которые могут стать известны компании в ходе данного интервью, т.к. кандидат может озвучить то, что он не указывал до этого в резюме.
7. При проведении телефонных интервью желательно сразу проинформировать кандидата о том, что, если он собирается сообщить какие-то дополнительные ПДн, то нам потребуется от него последующее согласие на уточнение предоставленных ранее ПДн, если он хочет, чтобы эти данные были занесены в его резюме в нашей базе данных и использовались для оценки на соответствие должности. Руководитель, проводящий интервью, должен быть проинструктирован, что задавать можно только те вопросы, которые касаются деловых качеств кандидата (ст. 3 ТК РФ), и никак не вопросы, которые затрагивают специальные категории персональных данных. Как минимум на это требуется письменное согласие, а как максимум это может быть расценено, как попытка дискриминации. Например, такие сведения, как вероисповедание, работодатель запрашивать не имеет права, так как они не требуются для выполнения трудовой функции.

Получение согласия на обработку персональных данных Роскомназор не разрешает, о чем указано в его ответах на официальном сайте <https://rkn.gov.ru/treatments/p459/p468/>

*«Получение согласия на обработку персональных данных по телефону, посредством СМС-сообщений действующим законодательством Российской Федерации не установлено.»*

1. При проведении интервью посредством видео-звонка кандидату руководитель также должен уведомить его обо всем вышеперечисленном. А если видео-звонок записывается, то обязан предупредить его об этом до начала записи и уже в самой записи кандидат должен озвучить, что он согласен на такую запись, а также назвать себя, чтобы его видеоизображение не стало относиться к биометрическим персональным данным, на обработку которых требуется его письменное согласие. Например, сразу в начале записи кандидат должен сказать: «Я, такой-то, в целях прохождения мною собеседования на вакантную должность такую-то даю свое согласие на запись данного видео и обработку его компанией такой-то до закрытия вакансии».

Этап третий – передача сведений, предоставленных кандидатом в службу безопасности.

1. Кандидат должен быть уведомлен рекрутером о том, как проходит процедура рассмотрения его на вакантную позицию, в том числе, что одним из этапов будет проверка информации службой безопасности. Этого же требует ч.4 ст. 18 № 152-ФЗ, чтобы освободить оператора от предоставления субъекту о получении ПДн не от него самого.

|  |  |
| --- | --- |
| **Требует уведомления кандидата** | **Не требует уведомления кандидата** |
| ч.3 ст.18 № 152-ФЗ | ч.4 ст.18 № 152-ФЗ |
| Если персональные данные получены не от субъекта персональных данных, оператор, за исключением случаев, предусмотренных частью 4 настоящей статьи, до начала обработки таких персональных данных обязан предоставить субъекту персональных данных следующую информацию: 1) наименование либо фамилия, имя, отчество и адрес оператора или его представителя; 2) цель обработки персональных данных и ее правовое основание; 3) предполагаемые пользователи персональных данных; 4) установленные настоящим Федеральным законом права субъекта персональных данных; 5) источник получения персональных данных. | Оператор освобождается от обязанности предоставить субъекту персональных данных сведения, предусмотренные частью 3 настоящей статьи, в случаях, если: 1) субъект персональных данных уведомлен об осуществлении обработки его персональных данных соответствующим оператором; ... 3) персональные данные сделаны общедоступными субъектом персональных данных или получены из общедоступного источника; |

1. Служба безопасности, как правило, хочет выявить факты, которые негативно влияют на выполнение соискателем своей трудовой функции. При этом они проверяют:

* Личные данные и документы. Ст. 65 ТК РФ содержит закрытый перечень документов, которые вправе потребовать работодатель при приеме и заключении трудового договора. Проверка подлинности представленных документов возможна различными способами. Действительность паспорта проверяют на сайте МВД, номер ИНН — через сайт ФНС, диплом — сделав запрос в учебное заведение, судимость легко проверяется через сайт суда общей юрисдикции, расположенного по адресу регистрации кандидата. Также в открытом доступе находится информация об административных штрафах, исполнительных производствах (сайт судебных приставов), о том, является ли человек учредителем какой-либо компании, и пр.

Правомерность проверки ряда таких документов представляется сомнительной, т.к. номер ИНН или наличие административных правонарушений никак не влияет на профессиональные качества кандидата. А вот диплом об образовании может являться требованием к его квалификации, поэтому такая проверка выглядит вполне резонной.

Поэтому рекомендуется строго ограничить перечень проверяемых данных.

* Трудовая биография. Представители службы звонят бывшим работодателям, а иногда и коллегам. Это позволяет выяснить реальные причины увольнения, особенности характера человека, его компетентность и отношения с коллегами.

Поскольку мы обязаны уведомить кандидата, если по своей инициативе будем звонить на его бывшие места работы, то предпочтительнее сразу получить от самого кандидата рекомендательные письма или контакты рекомендателей в резюме. Таким образом его согласие на обработку будет распространяться на эти данные в том числе. Делать это тайно незаконно.

* Информация из социальных сетей. Иногда изучение соцсетей, дает много информации о сотруднике и даже помогает составить его психологический портрет. Но, как мы уже видели, Роскомнадзор не считает такой сбор информации законным. Поэтому, если мы это и делаем для принятия каких-то решений, то никогда не храним никакие документы, связанные с такими «изысканиями», просто учитываем какую-то информацию при принятии решения.
* Во многих организациях при приеме проверяется кредитная история соискателя и наличие связей с конкурирующими организациями. Это также не имеет под собой легального основания.
* Проверка сведений о судимости абсолютно незаконна за исключением ряда случаев, которые прописывает закон.

*Отдельные работники при заключении трудового договора должны представить работодателю справку о наличии (отсутствии) судимости и (или) факта уголовного преследования либо о прекращении уголовного преследования по реабилитирующим основаниям (далее - справка об отсутствии судимости) (абз. 7 ч. 1 ст. 65 ТК РФ).*

*Эта справка выдается в порядке, предусмотренном Административным регламентом Министерства внутренних дел Российской Федерации по предоставлению государственной услуги по выдаче справок о наличии (отсутствии) судимости и (или) факта уголовного преследования либо о прекращении уголовного преследования (утв. Приказом МВД России от 07.11.2011 N 1121; далее - Административный регламент).*

*Справку можно передать работодателю как в бумажном виде, так и в электронном. Электронный документ должен быть заверен усиленной квалифицированной электронной подписью уполномоченного должностного лица МВД России (п. 83 Административного регламента).*

*Такую справку необходимо представлять при поступлении на работу, связанную с деятельностью, к осуществлению которой в соответствии с Трудовым кодексом РФ, иным федеральным законом не допускаются лица, имеющие или имевшие судимость, подвергающиеся или подвергавшиеся уголовному преследованию. Это следует из абз. 7 ч. 1 ст. 65 ТК РФ.*

*В частности, данную справку работодатель должен потребовать у лица, которое он намерен принять:*

*на работу, предполагающую осуществление педагогической деятельности. Это следует из совокупности абз. 7 ч. 1 ст. 65, абз. 3, 4 ч. 2 ст. 331 ТК РФ;*

*на работу, предполагающую осуществление трудовой деятельности в сфере образования, воспитания, развития несовершеннолетних, организации их отдыха и оздоровления, медицинского обеспечения, социальной защиты и социального обслуживания, в сфере детско-юношеского спорта, культуры и искусства с участием несовершеннолетних. Это следует из совокупности абз. 7 ч. 1 ст. 65, ч. 1 ст. 351.1 ТК РФ;*

*на должность специалиста авиационного персонала. Это следует из совокупности абз. 7 ч. 1 ст. 65 ТК РФ, абз. 2 п. 3 ст. 52 Воздушного кодекса РФ;*

*на работу, непосредственно связанную с обеспечением безопасности объектов топливно-энергетического комплекса. Данный вывод следует из совокупности абз. 7 ч. 1 ст. 65 ТК РФ, п. 1 ч. 1 ст. 10 Федерального закона от 21.07.2011 N 256-ФЗ;*

*на работу, непосредственно связанную с обеспечением транспортной безопасности. Такой вывод следует из совокупности абз. 7 ч. 1 ст. 65 ТК РФ, п. 1 ч. 1 ст. 10 Федерального закона от 09.02.2007 N 16-ФЗ.*

*За справкой об отсутствии судимости может обратиться сам работник или его уполномоченный представитель (п. 2 Административного регламента).*

*Ответ МВД по Республике Дагестан*

**Этап четвертый – трансграничная передача данных для топ-позиций.**

Трансграничную передачу данных регламентируют:

* ст.12 № 152-ФЗ;
* ч.5 ст.18 № 152-ФЗ;
* Конвенция Совета Европы о защите физических лиц при автоматизированной обработке персональных данных от 1981 г. ETS от 28.12.1981 г. № 108
* ст.1 Федерального закона от 21.07.2014 № 242-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях»

*«При сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети “Интернет”, оператор обязан обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации, за исключением случаев, указанных в пунктах 2, 3, 4, 8 части 1 статьи 6 настоящего Федерального закона».*

Что мы можем вынести из этих нормативных актов:

1. Трансграничная передача данных в страны, являющиеся сторонами Конвенции, а также в иные страны, которые в соответствии с приказом Роскомнадзора от 15.03.2013 № 274 признаны обеспечивающими адекватную защиту прав субъектов персональных данных, не требует письменного согласия субъекта ПДн, но по общему правилу требует информированного, осознанного согласия.
2. Трансграничная передача данных не запрещена.
3. Сбор ПДн, в том числе с территории иностранных государств, ведется только в базах данных на территории РФ. Стоит отметить, что требование распространяется только на обработку ПДн при их сборе, к тому же перечень видов обработки закрытый и неполный. Таким образом, можно сделать вывод о том, что последующие действия с ПДн могут производиться в базах данных (БД) на территории иностранных государств.
4. Объем и актуальность ПДн, хранящихся в БД на территории РФ, должны быть равны или превосходить соответствующие показатели в отношении ПДн, хранящихся в зарубежных БД.
5. Получение новых ПДн посредством использования (анализа) имеющихся ПДн, которые были собраны в БД на территории РФ и переданы за рубеж, может производиться с помощью зарубежных БД и без предварительной локализации в РФ.

*Согласно разъяснениям Роскомнадзора и Минкомсвязи, сбор ПДн – это процесс целенаправленного получения данных непосредственно от субъекта или привлеченных для этого третьих лиц. Обязанность по их локализации в БД на территории РФ возникает только в период сбора ПДн. Если, например, в зарубежной системе на основании собранных и локализованных в РФ данных о работнике определяется его грейд, делается вывод о необходимости направления работника на повышение квалификации или о его продвижении по службе, то такие ПДн нельзя рассматривать как получаемые во время сбора, т.е. они не были получены от субъекта или через уполномоченных оператором лиц.*

Минкомсвязи на своем сайте открыла раздел «Обработка и хранение персональных данных в РФ. Изменения с 1 сентября 2015 года». В нем предлагаются разъяснения и ответы на вопросы, подготовленные на основании информации, полученной от представителей бизнеса, научного сообщества и органов государственной власти (Совета Федерации, Минкомсвязи, Роскомнадзора).

<https://digital.gov.ru/ru/personaldata/>

Роскомнадзор в ноябре 2016 г. опубликовал свой [комментарий](https://pd.rkn.gov.ru/library/p195/" \t "_blank) к Закону № 242-ФЗ, хотя он не может считаться вполне официальным, т.к. Роскомнадзор не наделен полномочиями трактовать законодательство.

<https://pd.rkn.gov.ru/library/p195/>

|  |  |  |
| --- | --- | --- |
| **Позиция Государственно-правового управления Президента РФ** | **Позиция Роскомнадзора** | **Позиция Минкомсвязи** |
| - Обработка ПДн российских граждан должна осуществляться с использованием БД, находящихся на территории РФ, если только в конкретной ситуации не применимы случаи, указанные в п. 2, 3, 4, 8 ч. 1 ст. 6 Закона № 152-ФЗ. - В Законе № 242-ФЗ отсутствует упоминание о дублирующих БД или актуальных копиях данных. - Исходя из положений ч. 1 ст. 1 Закона № 242-ФЗ он распространяется на всех операторов. - Запреты, установленные в Законе № 242-ФЗ, распространяются и на те ПДн, которые были ранее переданы за пределы РФ. | - Роскомнадзор при проведении проверок опирается на определение БП с ПДн. Согласно ему БД можно считать таблицу в формате Excel, Word, в которой содержится информация о ПДн граждан или иным образом упорядоченный массив ПДн, в том числе поддающийся обработке при помощи ЭВМ3. - В Законе № 242-ФЗ отсутствует запрет на трансграничную передачу ПДн, так как ст. 12 Закона № 152-ФЗ не подверглась изменениям. Обработка ПДн посредством их передачи, в том числе на территорию иностранного государства, является трансграничной передачей. Допускается передача ПДн российских граждан, содержащихся в БД, находящихся в РФ, в том числе на территорию иностранных государств, в порядке и в соответствии с условиями, определенными законодательством о ПДн. - Нормы Закона № 152-ФЗ не применяются за пределами территории РФ. Зарубежная обработка ПДн регулируется нормативными правовыми актами тех стран, в которых она осуществляется. - Порядок определения оператором места нахождения БД с ПДн нормативно закрепляться не будет. - Формирование и актуализация БД с ПДн российских граждан должны осуществляться на территории РФ. Требования Закона № 242-ФЗ не позволяют осуществлять отдельные процедуры, в том числе «хранение ПДн» в БД на территории иностранного государства. - Каждый случай, в котором при сборе ПДн будет осуществляться одновременное хранение БД на территории РФ и иностранного государства, будет являться нарушением Закона № 242-ФЗ, поскольку оператор при сборе ПДн допустит их хранение в БД за пределами РФ. После сбора ПДн, т.е. после формирования БД на территории РФ, недопустимо изменение условий ее хранения путем переноса БД на территорию иностранного государства. - Операторы должны самостоятельно определять процедуру установления гражданства субъекта ПДн. Если у оператора возникли трудности или сомнения в правильной идентификации гражданства субъектов ПДн, то он может осуществлять хранение ПДн этих субъектов в БД, размещенных на территории РФ. | - Субъект ПДн имеет право дать согласие на обработку своих ПДн и предоставить их любому юридическому или физическому лицу, находящемуся как на территории РФ, так и за ее пределами. Оператор по-прежнему обладает правом поручить обработку ПДн иностранному лицу и осуществлять трансграничную передачу ПДн. Например, российские дочерние организации могут передавать ПДн своих работников в глобальные ИС (HR-системы, ERP-системы и т.п.), операторами которых являются иностранные материнские компании или иные организации. - ИСПДн может обладать географически распределенной структурой. Часть ее элементов может находиться за пределами РФ.  - Применение дублирующих БД, находящихся на территории РФ или за ее пределами, прямо не запрещено действующим законодательством РФ. - Нормы Закона № 152-ФЗ применимы только на территории РФ, а Конвенция о защите физических лиц при автоматизированной обработке персональных данных ETS от 28 января 1981 г. № 108 имеет приоритет над этим законом. Соответственно, иностранные лица не обязаны соблюдать его требования за пределами РФ, и они не подлежат юридической ответственности, предусмотренной действующим законодательством РФ. - Закон № 242-ФЗ обратной силы не имеет.  - Обработка ПДн для целей, не предусмотренных международным договором РФ или законом, может быть осуществлена оператором в рамках исполнения требований, предусмотренных ч. 5 ст. 18 Закона № 152-ФЗ, путем размещения в центрах обработки данных на территории РФ БД, содержащей ПДн граждан РФ, большего размера или аналогичного объему ПДн, передаваемому на территорию иностранного государства. |

Итак, в первую очередь, нам нужно убедиться, что система, в которой мы работаем, обеспечивает сбор данных на территории РФ, а сервера, на которые в последующем будет осуществляться трансграничная передача данных, находятся в странах сторонах Конвенции Совета Европы. (Нидерланды являются стороной Конвенции).

Мы работам в SAP, а это значит, что мы вряд ли имеем собственные серверы, а размещаем данные у провайдера. У провайдера можно разместить данные либо путем предоставления информационной системы (SaaS – Software as a Service), либо путем размещения собственной информационной системы на площадке провайдера (IaaS – Infrastructure as a Service, PaaS – Platform as a Service).

Для нас это первый вариант, мы приобретаем готовую систему.

К провайдеру, который в рамках нашего с ним договора становится обработчиком персональных данных, предъявляются несколько базовых требований:

1. Расширенное требование по соблюдению конфиденциальности размещаемых данных;
2. Наличие лицензии на защиту конфиденциальной информации, либо наличие подрядчика с такой лицензией;
3. Корректное описание предоставляемой услуги, обозначение целей обработки;
4. Опубликованная политика адекватной обработки персональных данных;
5. Наличие Акта классификации и Модели угроз.

Поскольку при таком порядке обработки только обработчик имеет возможность обеспечить определенные параметры защиты персональных данных, то в договоре с ним должно быть прямо указано, что технические меры защиты организуются обработчик в соответствии с Приказом ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

Желательно, чтобы у провайдера была лицензия по технической защите конфиденциальной информации (ТЗКИ).

По информационному сообщению ФСТЭК от 30.05.2012 г. № 240/22/2222 “По вопросу необходимости получения лицензии ФСТЭК России на деятельность по технической защите конфиденциальной информации” провайдер:

* обрабатывает ПДн не для собственных нужд;
* обеспечивает техническую защиту по поручению заказчика.

Согласно открытым источникам с 2015 компанией ООО «САП СНГ» *«на мощностях ЦОДа, располагающегося в Москве в Курчатовском институте и созданного совместно с «Ростелекомом», теперь размещены облачные решения SAP — Ariba (управление процессом закупок) и Success Factors (система управления кадровыми ресурсами). Это, по заявлению SAP, позволяет российским заказчикам компании хранить свои данные в соответствии с изменившимися требованиями российского закона о персональных данных.»*

Также на сайте fstec.ru опубликован Реестр лицензий на деятельность по технической защите конфиденциальной информации ООО «САП СНГ» имеет лицензию от 17.09.2014 № 2429.

В Государственном реестре сертифицированных средств защиты информации есть сертификат на программное изделие «Интегрированная платформа со встроенными средствами защиты от несанкционированного доступа SAP SUCCESS FACTORS HCM SUITE, версия 1» от 18.05.2015 № 3411.

Из всего этого мы можем сделать вывод, что система SAP соблюдает все требования к защите ПДн и является надежным инструментом в том числе для трансграничной передачи данных.

Однако, я напомню. что при трансграничной передаче рекомендуется пользоваться только этой системой и не пересылать ПДн кандидатов другими способами, а в особенности незащищенными каналами передачи данных.

В случае с иностранными кандидатами мы не обязаны собирать информацию о них на территории РФ, т.к. это касается только граждан РФ, поэтому такая информация может быть собрана напрямую в головном офисе в Нидерландах.

**Этап пятый – закрытие вакансии, предложение о работе или отказ.**

В случае, если мы готовы сделать предложение кандидату, вопросов нет. В случае, если мы не готовы сделать предложение кандидату, у нас есть два варианта:

- мы заносим его в кадровый резерв, и у нас уже есть на это его согласие;

- мы уничтожаем его ПДн в соответствии с требованиями законодательства сразу после закрытия вакансии или в течение 30 дней с момента официального выхода работника на эту позицию.

Тут есть один важный момент, поскольку объем резюме очень большой, есть риск забыть удалить какие-то данные, поэтому идеально будет каким-то образом настроить нашу базу данных резюме, чтобы она ежедневно показывала, какие из резюме в какой срок подлежат уничтожению.

**Основные риски, которые возникают на данный момент:**

ч.2 Федерального закона от 02.12.2019 № 405-ФЗ

*8. Невыполнение оператором при сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети "Интернет", предусмотренной законодательством Российской Федерации в области персональных данных обязанности по обеспечению записи, систематизации, накопления, хранения, уточнения (обновления, изменения) или извлечения персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации, -*

*влечет наложение административного штрафа на должностных лиц - от 100 000 до 200 000 рублей; на юридических лиц -* ***от 1 000 000 до 6 000 000 рублей.***

*9. Повторное совершение административного правонарушения, предусмотренного частью 8 настоящей статьи, -*

*влечет наложение административного штрафа на должностных лиц - от 500 000 до 800 000 рублей; на юридических лиц -* ***от 6 000 000 до 18 000 000 рублей****.*

**Ну и не такая впечатляющая подборка от КоАП.** Но в свете последних разъяснений Роскомнадзор также планирует штрафовать не за факт нарушения, а за каждый выявленный случай, так что в нашей компании, помноженное на количество обрабатываемой информации, это тоже приобретает угрожающие масштабы.

*Гражданин, должностное лицо или организация обрабатывают персональные данные в случаях, не предусмотренных законодательством*

Для должностных лиц – штраф от 5000 до 10 000 руб.

Для организаций – штраф от 30 000 до 50 000 руб.

ч. 1 ст. 13.11 КоАП

*Гражданин, должностное лицо или организация обрабатывают персональные данные без письменного согласия лица, когда такое согласие требует закон*

Для должностных лиц – штраф от 10 000 до 20 000 руб.

Для организаций – штраф от 15 000 до 75 000 руб.

ч. 2 ст. 13.11 КоАП

*Гражданин, должностное лицо, предприниматель или организация не опубликовали или не предоставили неограниченный доступ к документу с политикой по обработке персональных данных или сведениями по их защите*

Для должностных лиц – штраф от 3000 до 6000 руб.

Для организаций – штраф от 15 000 до 30 000 руб.

ч. 3 ст. 13.11 КоАП